

LN INTRUDER



Manual del Usuario Versión 1.00 (2012/08/15 – 16:33)

TABLA DE CONTENIDOS

1.	AVISOS LEGALES	3
2.	CARACTERÍSTICAS TÉCNICAS DEL LNIntruder	4
a.	Hardware:	4
b.	Software:	5
3.	NOTAS IMPORTANTES (Leer Primero !!!)	6
4.	PRIMEROS PASOS CON EL LNIntruder	7
5.	CONEXIÓN POR SSH (Línea de Comandos)	11
6.	CONCEPTOS BÁSICOS DE LOS TÚNELES CIFRADOS REMOTOS	12
1)	CONFIGURACIÓN:	12
2)	INSTALACIÓN IN-SITU:	13
3)	CONEXIÓN REMOTA (OWNING & PWINING !!!)	14
7.	CONFIGURACIÓN BÁSICA DEL SERVIDOR LNINTRUDER MASTER	16
8.	CONFIGURACIÓN LOCAL BÁSICA DEL MINISERVIDOR LNINTRUDER	19
9.	CONFIGURACIÓN DE TÚNELES CIFRADOS EN EL MINISERVIDOR LNINTRUDER	23
10.	RECEPCIÓN DE TÚNELES CIFRADOS EN EL SERVIDOR LNINTRUDER MASTER	24
11.	MONITOREO DEL ESTADO DE LOS TÚNELES CIFRADOS	28
12.	USO DE TARJETA DE ALMACENAMIENTO SDHC	29
13.	USO DEL MÓDEM 3G USB	30
14.	CONSIDERACIONES FINALES	32
a.	IPTables	32
b.	Servidor LNIntruder MASTER	32
15.	BACKUP Y RESTAURACIÓN DEL LNINTRUDER	33

1. AVISOS LEGALES

- Todos los productos LNIntruder, y demás productos desarrollados y/o distribuidos por LowNoise Hacking Group (LNHG – <http://www.lownoisehg.org/>) y/o Information Technology Security Solutions (ITSS), S.A.S. (<http://www.itss.com.co/>) son para ser empleados **ÚNICAMENTE** en actividades legales y autorizadas.
- Al usar este producto, el usuario está aceptando los términos del Contrato de Licencia de Usuario Final (CLUF) de ITSS, S.A.S. (<http://lnintruder.lownoisehg.org/CLUF.pdf>)
- Este producto contiene software propietario, así como software de código abierto (open-source software)
- La distribución del software propietario contenido en este producto está regido por los términos del Contrato de Licencia de Usuario Final (CLUF) de ITSS, S.A.S. (<http://lnintruder.lownoisehg.org/CLUF.pdf>)
- La distribución del software de código abierto (open-source software) contenido en este producto está regido por la Licencia Pública General de GNU (GNU GPL - <http://www.gnu.org/licenses/gpl.html>)
- Antes de la entrega al Usuario Final, cada uno de los equipos producidos ha sido evaluado, y cada funcionalidad ha sido puesta a prueba, tanto el sistema operativo, como la implementación de los túneles cifrados, y el uso de las interfaces cableada, inalámbrica (WiFi) y celular (3G/GSM), entre otras pruebas.
- El Usuario Final debe haber leído este documento (Manual del Usuario) en su totalidad antes de operar el producto por primera vez. De presentarse cualquier duda o inquietud con el contenido de este documento, favor comunicarse con el fabricante (lnintruder@lownoisehg.org) antes de poner en funcionamiento el producto.

2. CARACTERÍSTICAS TÉCNICAS DEL LNIntruder

a. Hardware:

Procesador:

ARM Marvell Kirkwood 88F6281 (ARM9E) a 1.2 GHz
L1 Cache: 16K Instruction + 16K Data
L2 Cache: 256KB

Memoria:

512 MB SDRAM
512 MB Flash

Potencia / Consumo:

Entrada: 100-240VAC/50-60Hz Max. 20W
Consumo DC: 5V/3.0A Max.
Consumo DC típico: 2.3W idle sin periféricos, 7.0W corriendo al 100% de uso de CPU
Convertidores DC-DC POL de alta eficiencia

Conectividad:

USB 2.0
Slot SD - Incluye Tarjeta SD 16GB Clase 10
Gigabit Ethernet
JTAG mini USB

Almacenamiento:

External hard drive
Tarjetas SDIO
Memoria Flash

Pantalla:

Ninguna

Dimensiones:

11.0cm (Largo) x 6.95cm (Ancho) x 4.85cm (Alto)

Tarjeta de Conectividad Wireless (WiFi):

Alfa Network 802.11b/g Long-Range Wireless USB Adapter
Modelo: AWUS036H

Módem USB de Conectividad 3G/GSM:

Módem USB Marca ZTE – Modelo: MF190S

Almacenamiento Externo:

Tarjeta SDHC de 16GB (Máxima Velocidad – Class 10 - 10 MB/s)

b. Software:

Sistema Operativo:

Linux Debian Squeeze 6.0.5

(<http://www.debian.org/News/2012/20120512>)

Sistema LNIntruder:

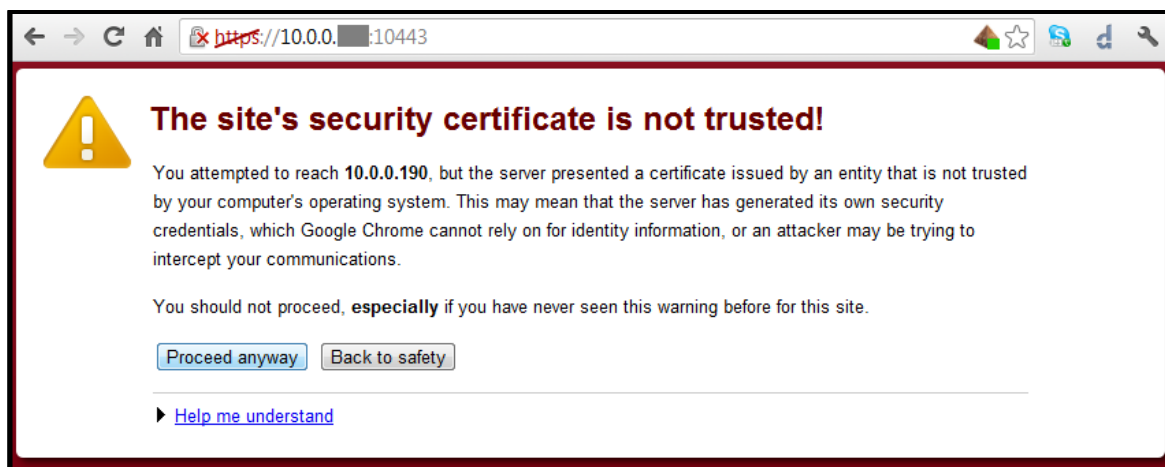
- Interfaz Web de configuración y monitoreo del sistema LNIntruder (Puede ser deshabilitada por el usuario)
- Levanta y mantiene activos túneles cifrados por diferentes protocolos IP (SSH, HTTP, SSL, DNS e ICMP), a través de diferentes interfaces de comunicación posibles (red cableada, red inalámbrica (WiFi) o red celular de datos (3G/GSM)). Estos túneles permiten acceso remoto a la red local conectada, desde cualquier lugar en Internet (o la red remota configurada)
- Todo el tráfico de montaje de los túneles y todo el tráfico transmitido a través de éstos viaja totalmente cifrado (OpenSSH/OpenSSL)
- De ser necesario, dependiendo de la configuración de red seleccionada, los túneles cifrados tienen la capacidad de atravesar firewalls, proxies y sistemas de detección de intrusos (IDS) al utilizar protocolos permitidos por la red atacada.
- Por defecto el miniservidor LNIntruder utiliza IPTables (firewall por software) para su protección y para dificultar su detección en redes atacadas.
- Software de evaluación de seguridad pre-instalado: nmap, metasploit, skipfish, w3af, dsniff, dnstracer, ettercap, wireshark, fping, hping3, iodine, nbtscan, nikto, sipcrack, socat, sqlmap, ike-scan, entre otros.
- Todo el software está en idioma Español.
- Fácil funcionamiento: Configure en casa, conecte en red a atacar, conéctese remotamente desde Internet. Eso es todo !

3. NOTAS IMPORTANTES (Leer Primero !!!)

- **POTENCIA USB:** El puerto USB del miniservidor LNIntruder sólo es capaz de entregar poca potencia debido a que su fuente de poder es bastante reducida. Si el Usuario Final desea conectar a este puerto más de un dispositivo USB de alta potencia (por ejemplo, un módem 3G/GSM Y una tarjeta WiFi USB) deberá proveerles energía de manera externa, por ejemplo, con un hub USB alimentado externamente con un adaptador.
- **CAPACIDAD DE PROCESAMIENTO:** El miniservidor LNIntruder cuenta con un procesador ARM Marvell Kirkwood 88F6281 (ARM9E), que funciona a una frecuencia de 1.2 GHz, lo cual lo hace poco eficiente para tareas que exijan una gran capacidad de procesamiento, como crackear passwords, cálculos matemáticos complejos o graficación avanzada, entre otros. En estos casos, se recomienda que se utilice el miniservidor LNIntruder como plataforma de recolección de datos, y éstos sean procesados más eficientemente de manera local en un computador de mayor potencia de procesamiento, para mejores resultados.
- **CAPACIDAD DE ALMACENAMIENTO:** El miniservidor LNIntruder cuenta con un almacenamiento interno de tan sólo 512MB, que al momento de enviar al Usuario Final, estará en un nivel de uso del 75% aproximadamente, siendo utilizado por el sistema operativo y algunos de los aplicativos de seguridad informática preinstalados. Para evitar llenar es espacio interno de almacenamiento, el miniservidor LNIntruder es entregado con una tarjeta SDHC de 16GB, como almacenamiento externo. En esta tarjeta están preinstalados algunos de los programas de seguridad informática que más espacio en disco consumen, y en esta tarjeta debe instalar el Usuario Final cualquier software adicional que desee adicionar al arsenal del LNIntruder. De ser necesario, el Usuario Final puede adquirir en el mercado tarjetas de almacenamiento SDHC de mayor capacidad (32GB, 64GB, etc.), verificando que cumplan con los requisitos de velocidad enunciados en la política de calidad del LNIntruder (deben ser Class 10, o sea, con una velocidad mínima de transmisión de datos de 10MB/s)

4. PRIMEROS PASOS CON EL LNIntruder

- 1) Conecte el LNIntruder a su red local (LAN) por medio de la interfaz cableada (eth0), y luego, préndalo, conectándolo a la red eléctrica.
- 2) Luego de aproximadamente un (1) minuto, el LNIntruder debe haber adquirido una dirección IP de la red, por medio del protocolo DHCP.
- 3) Identifique la dirección IP que el LNIntruder está utilizando (Puede mirar los logs de su servidor DHCP (o router), o escanear la red desde otro equipo en la misma LAN (por ejemplo, con nmap, teniendo en cuenta que el LNIntruder no responde a paquetes ICMP (ping), y sólo tiene abiertos los puertos 22 y 10443)
- 4) Ingrese a la Interfaz Web de Configuración y Monitoreo, en: [https://\[DirecciónIP\]:10443/](https://[DirecciónIP]:10443/), **utilizando como navegador Google Chrome o Mozilla Firefox (MS Internet Explorer no es compatible con la versión actual de nuestra Interfaz Web)**. Esta interfaz utiliza SSL, pero el certificado utilizado no está firmado por ninguna entidad conocida por su navegador, así que el Usuario Final recibirá una advertencia de su navegador, indicándole que el certificado ha sido firmado por el mismo LNIntruder. Ignore dicha advertencia. Ejemplo de advertencia (Google Chrome):



- 5) La Interfaz Web de Configuración y Monitoreo solicitará al Usuario Final el usuario y password para el ingreso al sistema. Por defecto, el usuario preconfigurado es **lnintruder**, y el password preconfigurado es **lnintruder**. (No confundir con el login y password de acceso por SSH, que son diferentes).

6) Aparecerá la página básica de inicio de la Interfaz Web, que presentará el estado de los túneles cifrados (de fábrica van deshabilitados y desconfigurados), y presentará al Usuario Final algunos datos básicos del sistema operativo, las interfaces de red, y su configuración. Un ejemplo de esta página básica se presenta a continuación (con todos los túneles cifrados ya activos):



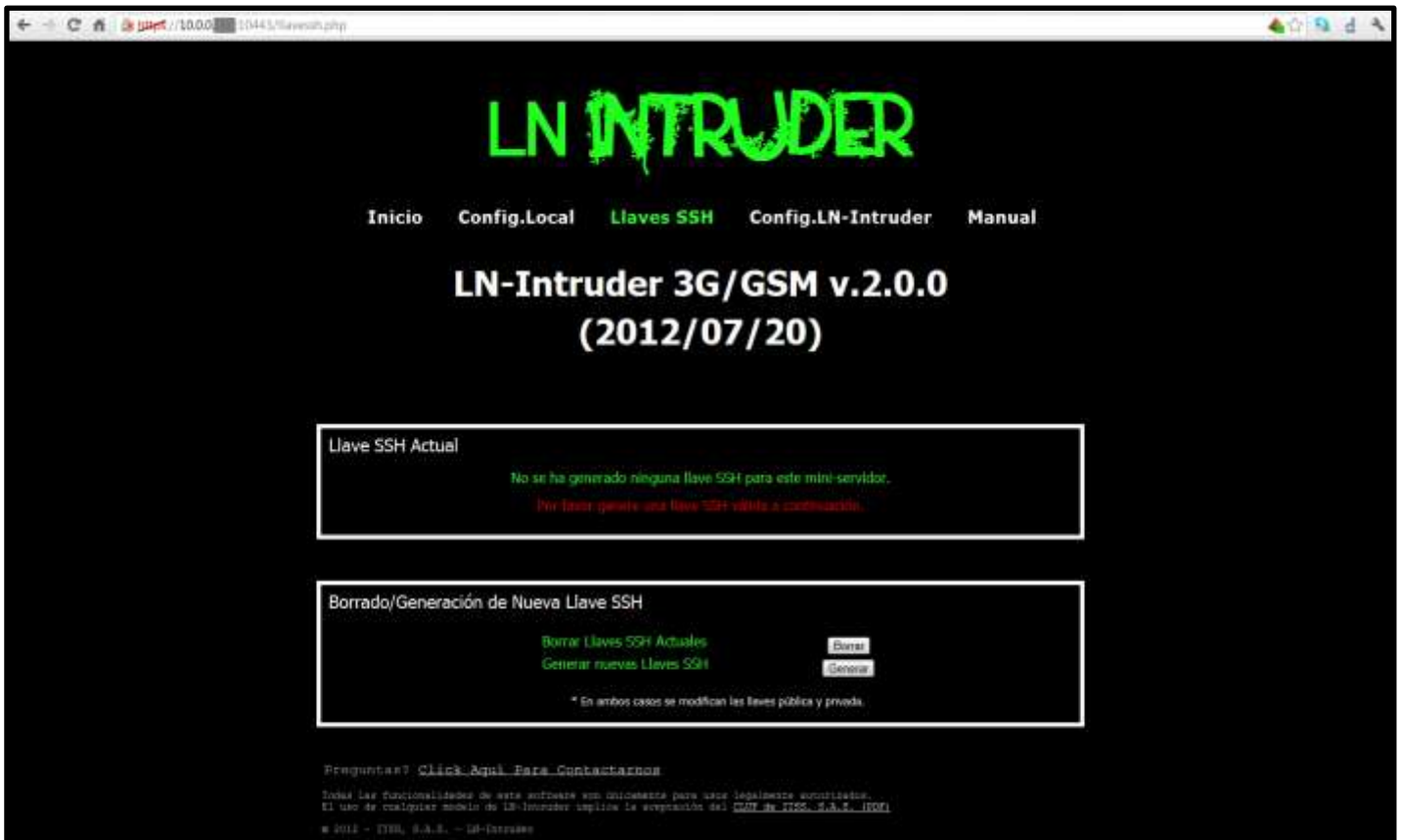
7) Utilice el menú superior para ingresar a la Configuración Local del miniservidor (Opción "Config.Local"). Aparecerá una página como la siguiente:



8) En esta página el Usuario Final podrá (opcionalmente):

- Cambiar el password de acceso a la Interfaz Web de Configuración y Monitoreo (El nombre de usuario siempre será **lnintruder**).
- Cambiar el nombre del miniservidor (Por defecto se llama **lnintruder**)
- Limpiar los Logs y Registros del Sistema
- Reiniciar el miniservidor LNIntruder
- Deshabilitar la Interfaz Web de Configuración y Monitoreo (al terminar la configuración, y antes de conectarlo en la red a atacar)
- Configurar TODOS los parámetros de las interfaces de red asociadas al miniservidor LNIntruder (eth0, wlan0 y/o ppp0)

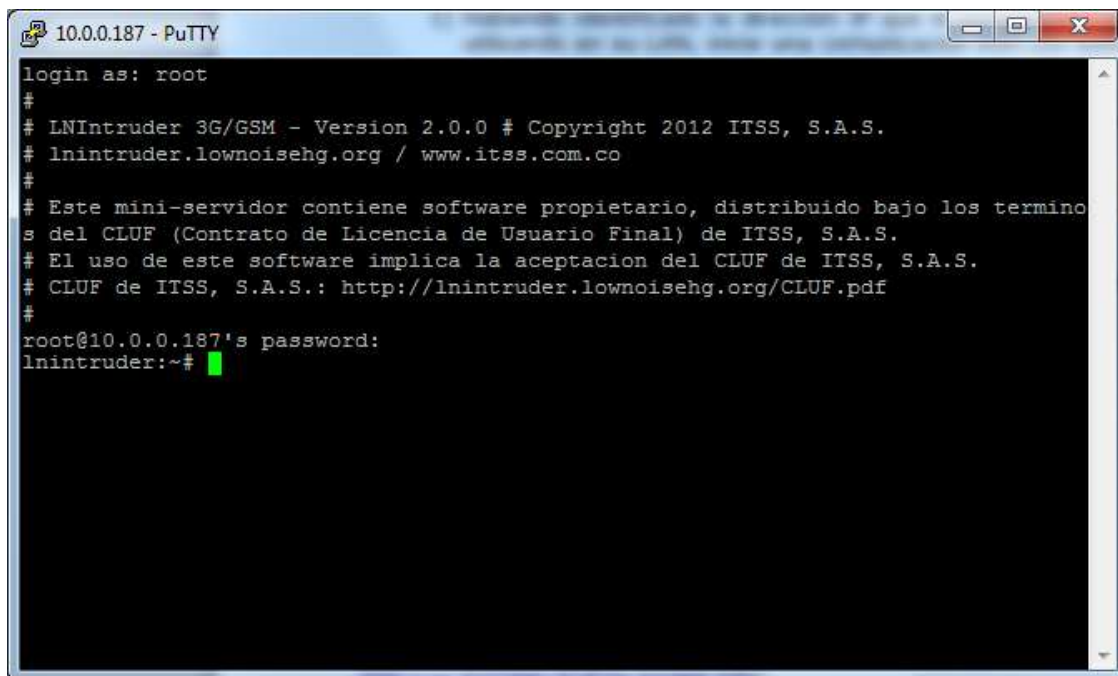
- 9) Utilice el menú superior para ingresar a la Configuración de Llaves SSH del miniservidor (Opción "Llaves SSH"). Aparecerá una página como la siguiente:



- 10) En esta página el Usuario Final podrá:
- Generar una llave SSH (única) para su miniservidor LNIntruder, que será utilizada (ver más adelante en CREACIÓN DE TÚNELES) para el establecimiento de las comunicaciones cifradas sin necesidad del ingreso de passwords o contraseñas.
 - Borrar la llave SSH existente, en caso de querer generar una nueva.

5. CONEXIÓN POR SSH (Línea de Comandos)

- 1) Habiendo identificado la dirección IP que el miniservidor LNIntruder está utilizando en su LAN, inicie una comunicación SSH con este (en Linux con el comando `ssh`, o en Windows con un cliente como *PuTTY* (<http://the.earth.li/~sgtatham/putty/latest/x86/putty-0.62-installer.exe>)), al puerto 22/tcp. El usuario administrador es **root** y el password por defecto es **LowNoiseHG**.



```
10.0.0.187 - PuTTY
login as: root
#
# LNIntruder 3G/GSM - Version 2.0.0 # Copyright 2012 ITSS, S.A.S.
# lnintruder.lownoisehg.org / www.itss.com.co
#
# Este mini-servidor contiene software propietario, distribuido bajo los termino
s del CLUF (Contrato de Licencia de Usuario Final) de ITSS, S.A.S.
# El uso de este software implica la aceptacion del CLUF de ITSS, S.A.S.
# CLUF de ITSS, S.A.S.: http://lnintruder.lownoisehg.org/CLUF.pdf
#
root@10.0.0.187's password:
lnintruder:~#
```

- 2) **NOTA IMPORTANTE:** El usuario administrador **root** tiene control **ILIMITADO** sobre el sistema operativo y todos sus parámetros. De no ser utilizado responsablemente, es posible destruir el sistema operativo y/o la configuración del mismo. Si no está seguro de lo que está haciendo, límitese a la configuración desde la Interfaz Web. Cualquier daño al software del sistema de túneles cifrados automáticos del LNIntruder o a la Interfaz Web de Configuración y Monitoreo causado por el usuario es su total responsabilidad, y su reinstalación/reconfiguración podrá tener costos no cubiertos por la compra del equipo.
- 3) Garantizando que su LNIntruder tenga acceso a Internet, actualice el sistema operativo y los aplicativos instalados con el comando:
apt-get update && apt-get upgrade -y
- 4) Actualice su instalación del Metasploit Framework:
cd /opt/metasploit-framework
git pull

- 5) Actualice su instalación de W3AF Framework:
cd /opt/w3af
svn update

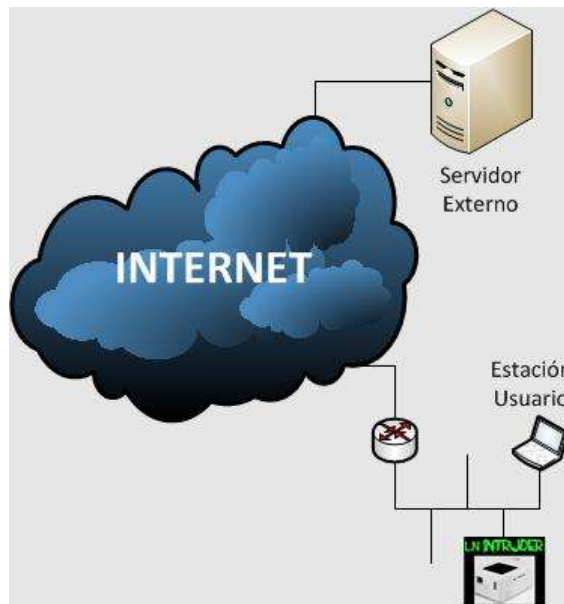
6. CONCEPTOS BÁSICOS DE LOS TÚNELES CIFRADOS REMOTOS

El concepto de "extrusión – intrusión hacia afuera", o "Hacking de 180 Grados" implementado en el LNItruder consiste en generar uno o varios túneles cifrados, desde una red interna (red atacada/evaluada) hasta un servidor externo (en Internet), controlado por el administrador del LNItruder. A través de este servidor externo, en Internet, desde este momento denominado el **LNItruder MASTER**, se tendrá acceso a los servicios y redes internas a las que tenga acceso el miniservidor LNItruder.

Bajo este principio, la utilización del miniservidor LNItruder es muy sencilla, y se define en los siguientes tres (3) pasos:

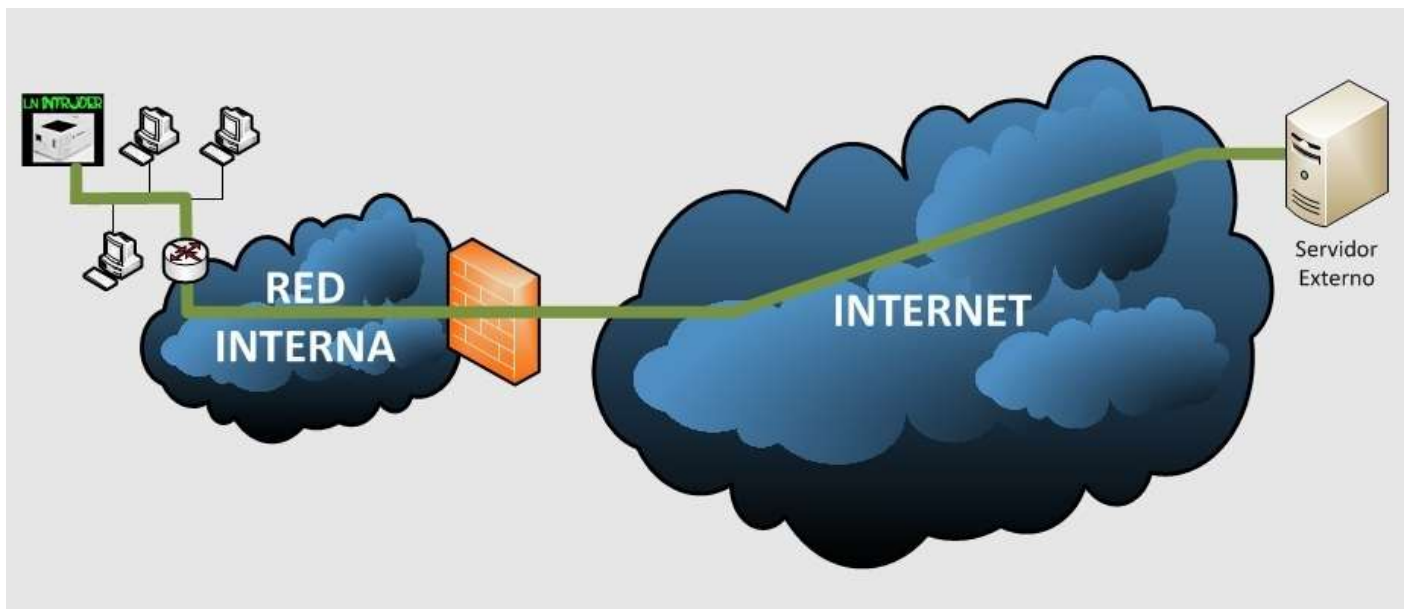
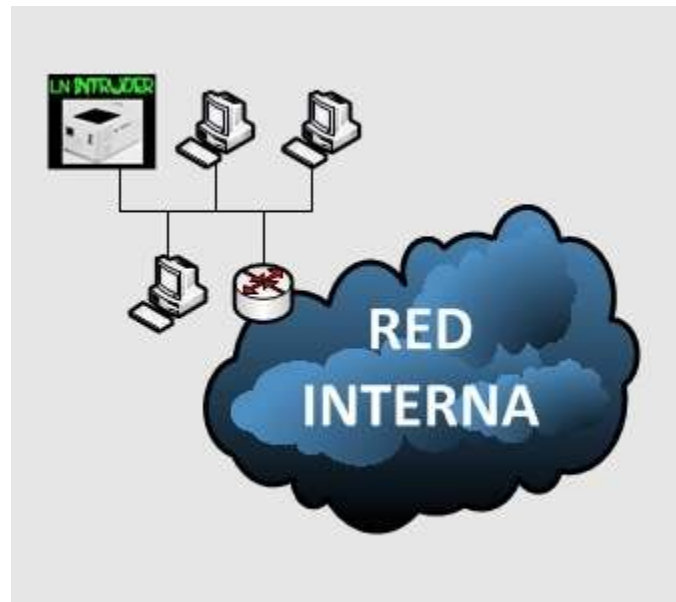
1) CONFIGURACIÓN:

- a. Se configura el servidor LNItruder MASTER (Ver Capítulos 7 y 10).
- b. Se configuran todos los parámetros del miniservidor LNItruder, de manera local (interfaces, redes, túneles, servicios, etc.), conectándolo directamente a un PC propio o en una LAN propia (casa, oficina, etc.) – (Ver Capítulos 8 y 9)



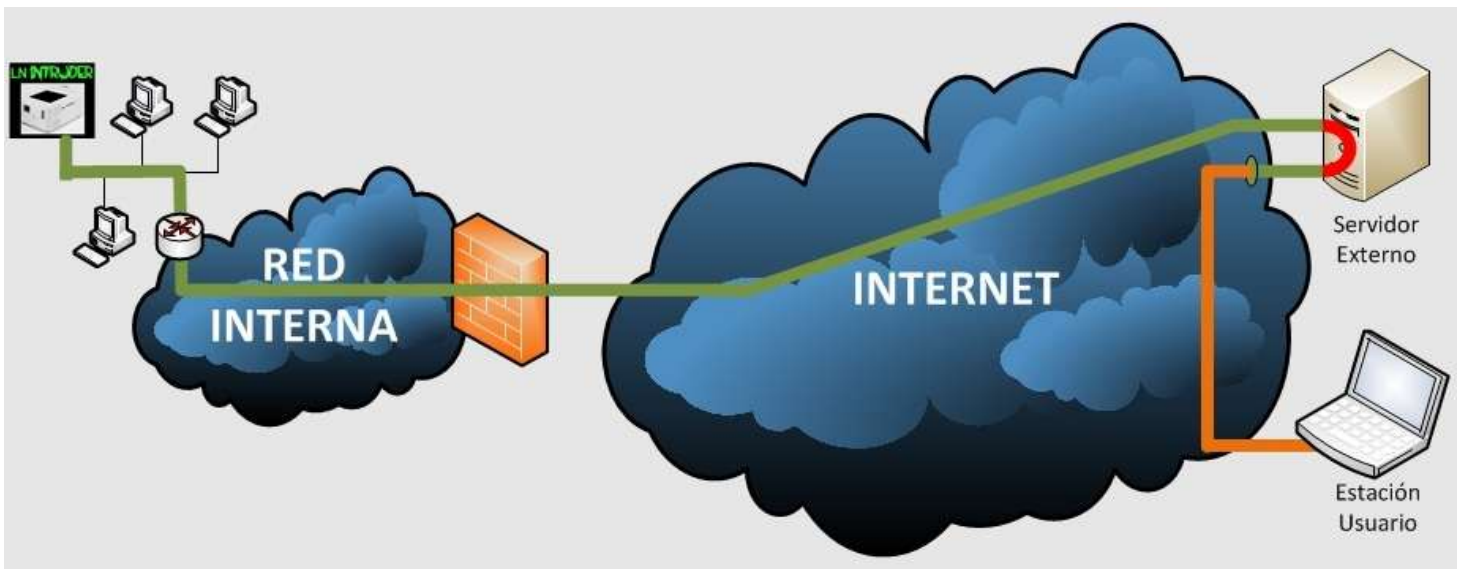
2) INSTALACIÓN IN-SITU:

- a. Se conecta el miniservidor LNIntruder a la red a ser atacada/evaluada, proveyéndole únicamente conexión de red (cableada, wireless, etc.) y energía eléctrica.
- b. El miniservidor LNIntruder identificará su red local, y generará en pocos minutos el túnel o túneles configurado(s) hacia el LNIntruder MASTER (por SSH, HTTP, SSL, DNS o ICMP).



3) CONEXIÓN REMOTA (OWNING & PWINING !!!)

- a. Desde la base de operaciones del evaluador/atacante (casa, oficina, etc.), o simplemente desde cualquier ubicación con acceso a Internet (conexión WiFi en un centro comercial, usando un módem 3G o un celular con plan de datos, etc.), se realizan las conexiones deseadas al miniservidor LNIntruder, a través del LNIntruder MASTER.
- b. Una vez conectado al miniservidor LNIntruder, podrás:
 - Ejecutar comandos sobre el miniservidor LNIntruder.
 - Identificar los equipos de red, servidores y estaciones de trabajo conectados a la red local a la que está conectado el miniservidor LNIntruder.
 - Identificar servicios y vulnerabilidades de todas las plataformas visibles desde el miniservidor LNIntruder.
 - Explotar remotamente las vulnerabilidades encontradas en todas las plataformas visibles desde el miniservidor LNIntruder.
 - Capturar tráfico sobre la red local a la que está conectado el miniservidor LNIntruder.
 - Infiltrar otras redes internas a través de la red local a la que está conectado el miniservidor LNIntruder.
 - Escalar el nivel de infiltración por medio de crackeo de passwords, captura de password viajando sin cifrado a través de la red, ataques de diccionario/fuerza bruta, ataques de ingeniería social a los usuarios de la red evaluada/atacada.
 - Y muchas otras ideas (hasta donde llegue la imaginación del evaluador/atacante) ...



NOTAS IMPORTANTES:

- Todos los túneles utilizan SSH (Secure SHell) como su medio de transporte y mecanismo de cifrado. Este protocolo es luego direccionado y/o encapsulado dentro de los otros protocolos soportados por el miniservidor LNIntruder (HTTP, SSL, DNS y ICMP) cuando es necesario. Por esta razón, es indispensable que el servidor LNIntruder MASTER tenga configurada la llave para conexiones SSH para la utilización de CUALQUIER tipo de túnel cifrado.
- Cada configuración de los cinco (5) tipos de túneles cifrados es independiente, por lo que se pueden diseñar túneles a diferentes direcciones IP (tener varios servidores LNIntruder MASTER) y utilizar los números de puerto que se desee para cada uno de ellos.
- El miniservidor LNIntruder intentará armar todos los túneles configurados (ya sea sólo uno, o los cinco), desde el momento que pueda conectarse a la red local. Es importante saber que la interfaz por la que se realizarán los túneles cifrados hacia el servidor LNIntruder MASER no siempre tiene que ser la misma que conecta al miniservidor LNIntruder a la red local atacada/evaluada.

EJEMPLO: Asumamos que la interfaz conectada a la red local atacada/evaluada es la red cableada (eth0)

- a. Si queremos armar los túneles cifrados por la misma red (eth0):** Nuestra salida a Internet será a través de la red local atacada/evaluada, por lo que seguramente deberemos evadir los mecanismo de seguridad perimetral hacia afuera que haya implementados (como un firewall, un router con ACLs, etc.). Para esto se usan los cinco tipos de túneles, ya que no es fácil obtener una configuración de filtrado de paquetes que bloquee el 100% de las comunicaciones salientes. El usuario deberá identificar la mejor manera de configurar sus túneles para cada caso en particular.
- b. Si queremos armar los túneles cifrados por la interfaz WiFi (wlan0):** Debemos identificar cual es nuestro camino de salida hacia Internet. Si es a través de una red wireless (WiFi) de la misma red atacada/evaluada, seguramente necesitaremos de las medidas de evasión explicadas en el punto anterior. Si por el contrario, estaremos conectados a una red inalámbrica (WiFi) pública, por ejemplo de una restaurante cercano, es probable que no necesitamos evadir firewalls, y con que un solo tipo de túnel sería suficiente.
- c. Si queremos armar los túneles cifrados por la interfaz 3G/GSM (ppp0):** Nuestra salida a Internet seguramente es a través de la red del operador celular seleccionado (el de la tarjeta SIM), y es muy probable que no necesitamos evadir firewalls, y que con un solo tipo de túnel sería suficiente.

7. CONFIGURACIÓN BÁSICA DEL SERVIDOR LNINTRUDER MASTER

Como ya se mencionó, el servidor LNIntruder MASTER es un servidor en Internet (con dirección IP Pública) bajo el control del administrador del miniservidor LNIntruder. Este servidor recibe los túneles cifrados armados por el miniservidor LNIntruder desde su locación remota, dentro de la red atacada/evaluada.

Todos los túneles cifrados utilizan SSH como medio de transporte de datos y como mecanismo de cifrado de los mismos. Por esta razón, lo primero que debemos configurar en el servidor LNIntruder MASTER es una cuenta de usuario y una llave de SSH para la conexión de dichos túneles cifrados.

Para este ejemplo, se presenta tal cuál se haría en Linux Debian o Ubuntu (y sistema operativos Linux basados en éstos, como BackTrack). Seguramente se puede configurar y hacer funcionar en otras versiones de Linux, y hasta en otros sistemas operativos (como MS Windows, Mac OS, etc.), pero hasta el momento eso no es soportado por los programadores/distribuidores del LNIntruder, ni está en los planes a futuro.

En la línea de comandos de un shell (por telnet, SSH, consola, etc.) sobre el servidor Linux donde se desea implementar el LNIntruder MASTER, ejecute los siguientes pasos, **como USUARIO 'root'**:

- 1) El servicio SSH debe estar instalado y corriendo.
 - a. Si no tiene instalado el servicio:
root@server:~# apt-get install openssh-server -y
 - b. Cuando ya esté instalado:
root@server:~# /usr/sbin/service ssh start
(para iniciar el servicio)
 - c. **NOTA:** Durante la instalación, o en el primer inicio del servicio, éste generará sus llaves y certificados de identificación y para el cifrado de datos.

- 2) Los túneles SSH cifrados (ya sea que estén encapsulados en cualquier protocolo soportado, o que se realicen de manera directa) utilizan una cuenta de usuario para dicha conexión. Para crear esta cuenta, realice los siguientes pasos en el servidor LNIntruder MASTER:
 - a. **root@server:~# /usr/sbin/useradd lnintruder -d /home/lnintruder -m**
 - b. **root@server:~# /bin/mkdir /home/lnintruder/.ssh**

- 3) Ya con la cuenta de usuario creada en el servidor LNIntruder MASTER, se debe copiar a ésta la llave SSH autorizada del miniservidor LNIntruder, para permitir la conexión SSH sin password. Siga los siguientes pasos:
- En la Interfaz Web de Configuración y Monitoreo del miniservidor LNIntruder (Ver Capítulo 4), ingrese a la opción "Llaves SSH", en el menú superior.



- Deberá aparecer la página de Configuración de Llave Pública y Llave Privada SSH.
- Bajo el título "Llave SSH Actual" se indica si aún estas llaves no han sido generadas, o se presenta la llave actual, si ya fueron generadas.
- Si aún no han sido generadas las llaves SSH, proceda a oprimir el botón "Generar" más abajo, en el título "Borrado/Generación de Nueva Llave SSH". Este proceso de generación debe durar unos 5-10 segundos aproximadamente. Inmediatamente, aparecerá la nueva llave en el título "Llave SSH Actual", en letra de color verde, y dentro de un cuadro de texto, como se muestra a continuación:



- e. Haga triple-click sobre el texto de la llave generada, de forma que quede seleccionada toda – desde su inicio (ssh-rsa...), hasta su final (...root@lnintruder).
- f. Copie dicho texto (Ctrl-C)
- g. De regreso en el shell de root sobre el servidor LNIntruder MASTER:
 - i. Edite el archivo /home/lnintruder/.ssh/authorized_keys
root@server:~# vim /home/lnintruder/.ssh/authorized_keys
 - ii. Oprima la tecla `i` para poder insertar texto en el archive (abajo debe aparecer la inscripción "-- INSERT --")
 - iii. Pegue (Click derecho del mouse) la llave copiada en el paso f.
 - iv. Oprima la tecla Escape (ESC) para detener el ingreso de texto.
 - v. Oprima `:qw!` (sin las comillas, es decir, dos puntos, la letra `q`, la letra `w`, el signo de admiración y la tecla ENTER), para guardar los cambios y salir.
 - vi. Ejecute los siguientes dos (2) comandos, en el shell, como usuario `root`:

root@server:~# chown -R lnintruder.lnintruder /home/lnintruder/.ssh

root@server:~# chmod 600 /home/lnintruder/.ssh/authorized_keys

8. CONFIGURACIÓN LOCAL BÁSICA DEL MINISERVIDOR LNINTRUDER

En este Capítulo del Manual, se detalla el funcionamiento de los parámetros configurables de la Interfaz Web de Configuración y Monitoreo en su opción "Config.Local" del menú superior.

Las opciones configurables en esta página son:

1) Cambio de Password de acceso a la Interfaz Web:



Cambiar Password de la Consola de Administración Web (Usuario: lnintruder)

Nuevo Password:

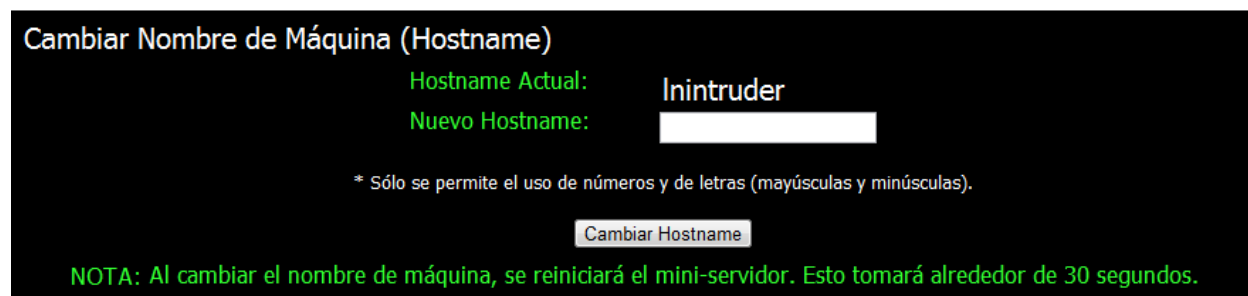
Nuevo Password (otra vez):

* Sólo se permite el uso de números y de letras (mayúsculas y minúsculas).

NOTA: Al cambiar el password, se reiniciará la interfaz web y se le solicitará loguearse nuevamente, con el nuevo password.

En esta sección, el Usuario Final puede cambiar el password de acceso a la Interfaz Web (el nombre de usuario siempre será 'lnintruder'). Se debe ingresar dos veces el nuevo password deseado (una en cada caja) y oprimir el botón "Cambiar Password". Se hará una verificación y se indicará si el password fue cambiado exitosamente. El password por defecto que trae de fábrica es **lnintruder**.

2) Cambio de Nombre de Máquina:



Cambiar Nombre de Máquina (Hostname)

Hostname Actual: lnintruder

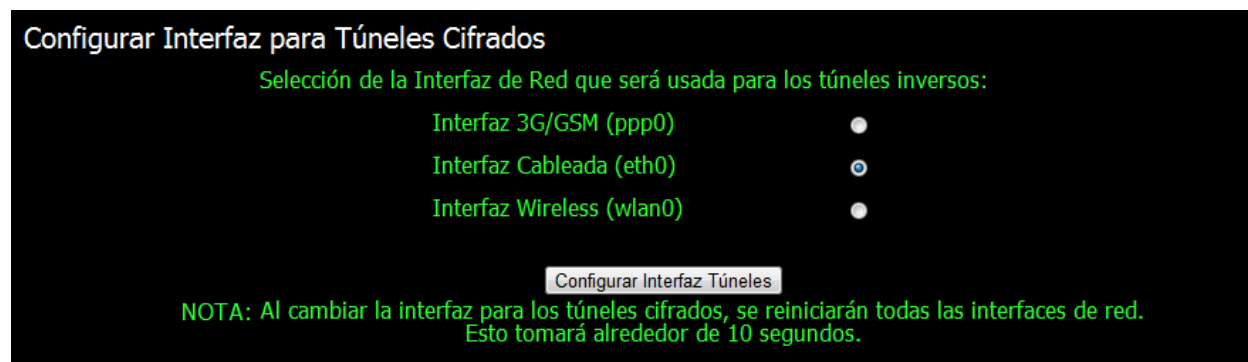
Nuevo Hostname:

* Sólo se permite el uso de números y de letras (mayúsculas y minúsculas).

NOTA: Al cambiar el nombre de máquina, se reiniciará el mini-servidor. Esto tomará alrededor de 30 segundos.

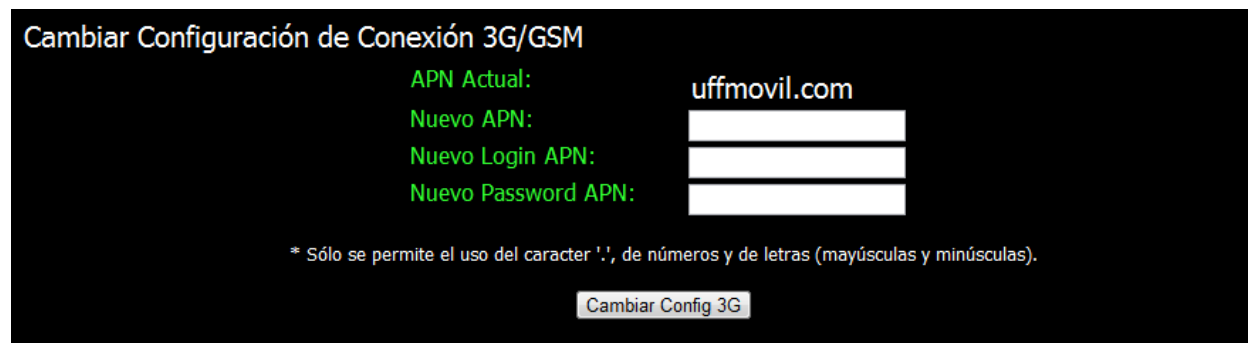
En esta sección, el Usuario Final puede cambiar el nombre de máquina del miniservidor LNIntruder. Se debe ingresar el nuevo nombre de máquina deseado en la caja, y oprimir el botón "Cambiar Hostname". Se hará una verificación y se indicará si el nombre de máquina fue cambiado exitosamente. El nombre de máquina por defecto que el miniservidor trae de fábrica es **lnintruder**.

3) Selección de la Interfaz para Túneles Cifrados:



En esta sección, el Usuario Final puede seleccionar por cual interfaz de red se generarán los túneles cifrados hacia el servidor LNIntruder MASTER, en Internet. Es importante resaltar que esta interfaz puede o no ser la misma que hará la conexión a la red atacada/evaluada. Seleccione la interfaz por la que el miniservidor LNIntruder tendrá acceso a Internet cuando ya esté instalado en la red atacada/evaluada, y oprima el botón "Configurar Interfaz Túneles". Los servicios de red del miniservidor serán reiniciados. Este proceso puede durar unos 10-30 segundos, y posteriormente se mostrará una pantalla de estado (éxito o falla).

4) Cambio de Parámetros de Conexión 3G/GSM:



En esta sección, el Usuario Final puede configurar todos los parámetros necesarios para la conexión a la red de datos del operador celular de su preferencia (del que el Usuario Final debe conseguir una tarjeta SIM). La tarjeta SIM debe contar con un plan de datos. No se necesita que el módem 3G esté conectado para esta configuración.

En las cajas de texto proveídas, se deben ingresar respectivamente el nombre del APN (Access Point Name) del operador celular, y el usuario y el password de dicho APN. Estos datos son facilitados por su operador celular en la línea de Soporte Técnico, o pueden ser fácilmente encontrados en Internet (i.e. Buscar en Google: "<operador> APN configuración").

Se deben ingresar esos datos y oprimir el botón "Cambiar Config 3G". Se hará una verificación y se indicará si el cambio fue exitoso o fallido.

5) Configuración de Red:



Configuración de Red

Configuración Interfaz Cableada (eth0)

Dirección IP Dinámica Asignada por DHCP (Recomendado)

Dirección IP Estática

Configuración Interfaz Wireless (wlan0)

No configurar ninguna Red Wireless:

Red Wireless SIN cifrado:

Red Wireless con cifrado WEP:

Red Wireless con cifrado WPA/WPA2:

Actualizar Configuración de Red

NOTA: Al cambiar el esquema de direccionamiento IP, se reiniciará el mini-servidor. Esto tomará alrededor de 30 segundos.

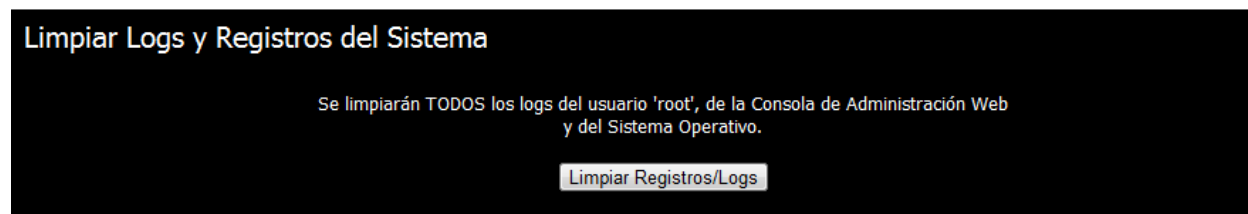
En esta sección, el Usuario Final puede configurar los parámetros de red de las interfaces cableada (eth0) y wireless/inalámbrica (wlan0). En ambos casos, se podrá seleccionar si el direccionamiento IP se trabajará de manera estática, o si será asignado por un servidor DHCP.

En el caso de la red inalámbrica, se puede seleccionar el tipo de cifrado configurado (ninguno, WEP, WPA o WPA2), ingresando los datos necesarios (nombre del ESSID, password, etc.)

Luego de ingresar todos los datos solicitados, se debe oprimir el botón "Actualizar Configuración de Red", se efectuará una verificación, y se reiniciará el miniservidor LNIntruder si todo está en orden. Este proceso puede tomar unos 30 segundos.

NOTA IMPORTANTE: No es necesario tener conectada la tarjeta de red inalámbrica USB al miniservidor LNIntruder para esta configuración. Cuando se desee utilizar dicha tarjeta de red inalámbrica con la configuración almacenada, se recomienda conectar el dispositivo USB desde **ANTES** de prender el miniservidor.

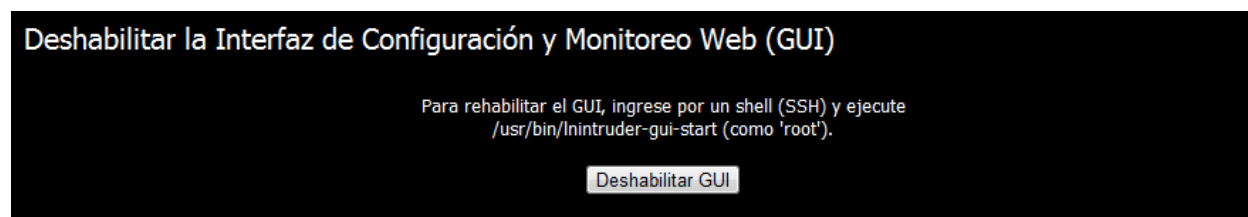
6) Limpieza de Logs y Registros del Sistema:



En esta sección, el Usuario Final puede limpiar y borrar todo registro de actividad (Interfaz Web, sesiones de Shell, etc.) del miniservidor LNIntruder. Los registros quedarán totalmente en blanco, tal cual el sistema sale de fábrica.

Al oprimir el botón "Limpiar Registros/Logs" se realizará una verificación, se limpiarán los logs y se presentará un estado de éxito o fallo de la solicitud.

7) Deshabilitado de la Interfaz Web:

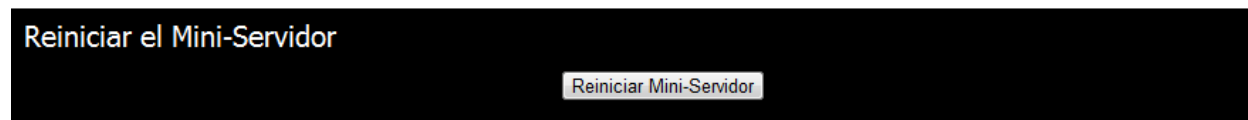


En esta sección, el Usuario Final puede deshabilitar totalmente el acceso Web (puerto 10443/tcp) a la Interfaz de Configuración y Monitoreo. Esto es recomendable luego de terminar la configuración local (Capítulo 6, Sección 1), ya cuando el miniservidor queda listo para su instalación en la red atacada/evaluada, para prevenir su fácil detección.

Para rehabilitar el servicio posteriormente, se debe ingresar a un Shell, como usuario 'root', y ejecutar:

```
root@server:~# /usr/bin/lnintruder-gui-start
```

8) Reinicio del Miniservidor LNIntruder:



En esta sección, el Usuario Final puede reiniciar el miniservidor LNIntruder, oprimiendo el botón "Reiniciar Mini-Servidor". El reinicio tomará unos 30 segundos.

9. CONFIGURACIÓN DE TÚNELES CIFRADOS EN EL MINISERVIDOR LNINTRUDER

En este Capítulo del Manual, se detalla el funcionamiento de los parámetros configurables de la Interfaz Web de Configuración y Monitoreo en su opción "Config.LN-Intruder" del menú superior. Estos parámetros corresponden a la configuración de los túneles cifrados de conexión hacia el(los) servidor(es) LNIntruder MASTER, en Internet.

Las opciones configurables en esta página son:

Configuración de Túneles Inversos SSH

Túnel Inverso Tipo I (SSH Puro):
 Activar
Dirección IP del Servidor Externo: Puerto TCP (0-65535):

Túnel Inverso Tipo II (SSH sobre HTTP):
 Activar
Dirección IP del Servidor Externo: Puerto TCP (0-65535):

Túnel Inverso Tipo III (SSH sobre SSL - HTTPS):
 Activar
Dirección IP del Servidor Externo: Puerto TCP (0-65535):

Túnel Inverso Tipo IV (SSH sobre DNS):
 Activar
Dirección IP del Servidor Externo: Puerto por defecto: 53/udp

Túnel Inverso Tipo V (SSH sobre ICMP):
 Activar
Dirección IP del Servidor Externo: Protocolo: ICMP (No hay puerto TCP/UDP)

* Revise cuidadosamente los datos ingresados. Los caracteres inválidos serán removidos.

En esta sección, para cada tipo de túnel, el Usuario Final podrá configurar la dirección IP del servidor LNIntruder MASTER a utilizar, y el puerto de los tres primeros tipos de túneles (TCP).

Igualmente, el Usuario Final podrá seleccionar cuáles túneles desea activar y cuáles no.

Todos los demás parámetros están automáticamente configurados, y solamente es necesario oprimir el botón "Generar Nueva Configuración" al terminr la configuración de direcciones IP y puertos TCP.

10. RECEPCIÓN DE TÚNELES CIFRADOS EN EL SERVIDOR LNINTRUDER MASTER

Cada tipo de túnel requiere algún servicio y/o software que esté esperando la comunicación y sepa cómo atenderla y entenderla. A continuación se presenta la configuración necesaria (en el servidor LNIntruder MASTER) para poder recibir cada tipo de túnel capaz de ser armado por el miniservidor LNIntruder:

1) Túnel SSH (SSH puro):

Para este tipo de túnel, solamente se necesita que el puerto de SSH (por defecto, el 22/tcp) del LNIntruder MASTER sea visible desde Internet en la dirección IP configurada. Este puerto puede ser cambiado, de acuerdo a lo visto en el Capítulo anterior del Manual.

En el servidor LNIntruder MASTER se puede verificar si el túnel está arriba con el siguiente comando (en un Shell, como usuario `root`):

```
root@server:~# /bin/netstat -an | grep 10001
```

Si el túnel está abajo, no debe aparecer nada. Si el túnel esta conectado, debe aparecer algo como:

```
tcp      0      0 127.0.0.1:10001    0.0.0.0:*          LISTEN
```

2) Túnel HTTP (SSH sobre HTTP):

Para este tipo de túnel, se debe estar corriendo el software httptunnel, que ya está instalado en Backtrack, y que puede ser fácilmente instalado en Debian/Ubuntu con el comando (en un Shell, como `root`):

```
root@server:~# apt-get install httptunnel -y
```

Cuando el software ya esté instalado, debe estar corriendo, a partir del siguiente comando:

```
root@server:~# /usr/bin/hts -F 0.0.0.0:22 80 &
```

Si Ud. configura el miniservidor LNIntruder para manejar este túnel (Tipo II) en otro puerto, remplace el "80" al final del comando por el número de puerto que seleccionó.

En el servidor LNItruder MASTER se puede verificar si el túnel está arriba con el siguiente comando (en un Shell, como usuario `root`):

```
root@server:~# /bin/netstat -an | grep 10002
```

Si el túnel está abajo, no debe aparecer nada. Si el túnel esta conectado, debe aparecer algo como:

```
tcp      0      0 127.0.0.1:10002    0.0.0.0:*          LISTEN
```

3) Túnel SSL (SSH sobre HTTPS):

Para este tipo de túnel, se debe estar corriendo el software stunnel, que ya está instalado en Backtrack, y que puede ser fácilmente instalado en Debian/Ubuntu con el comando (en un Shell, como `root`):

```
root@server:~# apt-get install stunnel -y
```

Para correr este software, y emular un servicio con SSL, se debe primero haber creado un certificado para el servicio. Si no lo ha hecho anteriormente, lo puede hacer con los siguientes comandos:

```
root@server:~# cd /root  
root@server:~# openssl genrsa -out lnintruder_key.pem 2048  
root@server:~# openssl req -new -key lnintruder_key.pem -out  
lnintruder.csr (Oprimir ENTER para todas las preguntas)  
root@server:~# openssl x509 -req -in lnintruder.csr -out  
lnintruder.crt.pem -signkey lnintruder_key.pem -days 1825  
root@server:~# cat lnintruder.crt.pem >> lnintruder_key.pem
```

Cuando el software ya esté instalado, y el certificado creado, se debe poner a correr, a partir del siguiente comando:

```
root@server:~# /usr/bin/stunnel -p /root/lnintruder_key.pem -d 443 -r  
localhost:22 &
```

Si Ud. configura el miniservidor LNItruder para manejar este túnel (Tipo III) en otro puerto, remplace el "443" en el comando por el número de puerto que seleccionó.

En el servidor LNItruder MASTER se puede verificar si el túnel está arriba con el siguiente comando (en un Shell, como usuario `root`):

```
root@server:~# /bin/netstat -an | grep 10003
```

Si el túnel está abajo, no debe aparecer nada. Si el túnel esta conectado, debe aparecer algo como:

```
tcp    0    0 127.0.0.1:10003    0.0.0.0:*    LISTEN
```

4) Túnel DNS (SSH sobre DNS):

Para este tipo de túnel, se debe estar corriendo el software dns2tcp. No se recomienda la versión instalada en Backtrack, ni la versión disponible por apt-get en Debian/Ubuntu. Se recomienda utilizar la última versión, descargando y compilando el código fuente con los siguientes comandos (en un Shell, como 'root'):

```
root@server:~# cd /root  
root@server:~# wget  
http://www.hsc.fr/ressources/outils/dns2tcp/download/dns2tcp-0.5.2.tar.gz  
root@server:~# tar -zxvf dns2tcp-0.5.2.tar.gz  
root@server:~# cd dns2tcp-0.5.2  
root@server:~# ./configure  
root@server:~# make
```

Para correr este software, se debe primero generar el archivo de configuración **/root/dns2tcpdrc**, con el siguiente contenido:

```
listen = 0.0.0.0  
port = 53  
user = nobody  
chroot = /var/empty/dns2tcp/  
domain = lnintruder.tv  
resources = ssh:127.0.0.1:22
```

NOTA: Asegúrese de que el directorio **/var/empty/dns2tcp/** exista, sino, créelo (con el comando: **mkdir -p /var/empty/dns2tcp**)

Cuando el software ya esté instalado, y el archivo de configuración esté listo, se debe poner a correr, a partir del siguiente comando:

```
root@server:~# /usr/local/bin/dns2tcpd -F -d 1 -f /root/dns2tcpdrc &
```

En el servidor LNIntruder MASTER se puede verificar si el túnel está arriba con el siguiente comando (en un Shell, como usuario 'root'):

```
root@server:~# /bin/netstat -an | grep 10004
```

Si el túnel está abajo, no debe aparecer nada. Si el túnel esta conectado, debe aparecer algo como:

```
tcp    0    0 127.0.0.1:10004    0.0.0.0:*    LISTEN
```

5) Túnel ICMP (SSH sobre ICMP):

Para este tipo de túnel, se debe estar corriendo el software ptunnel, que ya está instalado en Backtrack, y que puede ser fácilmente instalado en Debian/Ubuntu con el comando (en un Shell, como `root`):

```
root@server:~# apt-get install ptunnel -y
```

Cuando el software ya esté instalado, se debe poner a correr, a partir del siguiente comando:

```
root@server:~# /usr/bin/ptunnel &
```

En el servidor LNIntruder MASTER se puede verificar si el túnel está arriba con el siguiente comando (en un Shell, como usuario `root`):

```
root@server:~# /bin/netstat -an | grep 10005
```

Si el túnel está abajo, no debe aparecer nada. Si el túnel esta conectado, debe aparecer algo como:

```
tcp    0    0 127.0.0.1:10005    0.0.0.0:*    LISTEN
```

11. MONITOREO DEL ESTADO DE LOS TÚNELES CIFRADOS

Ya se mostró en el Capítulo anterior como verificar desde una consola de Shell del servidor LNItruder MASTER el estado de cada túnel, en caso de no tener acceso a la Interfaz Web de Configuración y Monitoreo (por ejemplo, ya cuando el miniservidor LNItruder está instalado en la red atacada/evaluada).

Si la Interfaz Web se deja prendida, y durante la fase de pruebas de los túneles, antes de su instalación en la red atacada/evaluada, se puede utilizar la página de monitoreo de dicha Interfaz Web, para conocer el estado de cada túnel. Esta información se presenta directamente en la página de inicio del portal web, o yendo a la opción "Inicio" del menú superior. Ejemplo:

```
Shells Inversos (SSH)
Conexión Inversa - SSH Directo: Sin Configurar
Conexión Inversa - Túnel HTTP: Configurado - Desconectado
Conexión Inversa - Túnel SSL (HTTPS): Sin Configurar
Conexión Inversa - Túnel DNS: Configurado - Conectado a 10.0.0.2:53/udp (Puerto remoto 10004/tcp)
Conexión Inversa - Túnel ICMP: Configurado - Conectado a 10.0.0.2/icmp (Puerto remoto 10005/tcp)
Estado Módem USB 3G/GSM: Desconectado
Conexión 3G/GSM a Internet: Desconectado
```

En esta sección del portal Web, se presenta el estado de los túneles como:

- a) Sin Configurar: El túnel no está activo en la configuración de túneles (Ver Capítulo 9)
- b) Configurado – Desconectado: El túnel está activo y configurado, pero no se ha dado conexión con el otro extremo (servidor LNItruder MASTER)
- c) Configurado – Conectado: El túnel está establecido con el servidor LNItruder MASTER (indica la dirección IP y puerto con que se hizo la primera comunicación, y el puerto en el que está activo el túnel en el otro extremo (LNItruder MASTER))

También se puede encontrar en esta sección información de la comunicación 3G/GSM. Ejemplo:

```
Shells Inversos (SSH)
Conexión Inversa - SSH Directo:      Configurado - Conectado a 23.█:22 (Puerto remoto 10001/tcp)
Conexión Inversa - Túnel HTTP:       Sin Configurar
Conexión Inversa - Túnel SSL (HTTPS): Sin Configurar
Conexión Inversa - Túnel DNS:        Sin Configurar
Conexión Inversa - Túnel ICMP:       Sin Configurar
Estado Módem USB 3G/GSM:             Conectado (Modelo: ZTE MF190 proveido con el LNIntruder)
Conexión 3G/GSM a Internet:          Conectado (Dirección IP: 190.29.█)
```

- a) Estado del Módem 3G/GSM:
 - a. Desconectado: No está conectado el módem al puerto USB
 - b. Conectado: El módem 3G proporcionado está conectado en el puerto USB (Se indica el modelo)
- b) Conexión 3G/GSM a Internet:
 - a. Desconectado: No hay conexión a Internet a través del Módem USB
 - b. Conectado: Hay conexión a Internet a través del módem USB 3G (y se indica la dirección IP que se obtuvo del operador celular en internet)

12. USO DE TARJETA DE ALMACENAMIENTO SDHC

Para utilizar una tarjeta de almacenamiento Secure Digital High Capacity (SDHC), ya sea la proveída con el equipo (16GB – Class 10) u otra, se recomienda que ésta sea conectada al dispositivo **ANTES** de prenderlo. La primera partición de la Tarjeta SDHC será montada automáticamente en el directorio /opt del sistema operativo. Otras particiones tendrán que ser montadas manualmente.

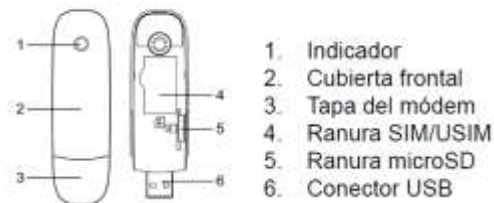
Si el Usuario Final desea adquirir otra(s) tarjeta(s) de almacenamiento, se recomienda que sean de velocidad igual o superior a la proveída (10 MB/s, o sea Class 10 o superior)

13. USO DEL MÓDEM 3G USB

El LNIntruder trae dentro de su kit un módem USB 3G, marca ZTE, modelo MF190S. Este módem está desbloqueado y puede ser utilizado con cualquier operador celular 3G/GSM de más de 160 países del mundo.

Conociendo su dispositivo

La siguiente figura muestra la apariencia del MF190. Es solo para su referencia, el producto actual puede ser diferente.



Para mayor información sobre los operadores celulares de los países del continente americano, consulte:

http://en.wikipedia.org/wiki/List_of_mobile_network_operators_of_the_Americas

Para mayor información sobre los operadores celulares de los países del continente europeo, consulte:

http://en.wikipedia.org/wiki/List_of_mobile_network_operators_of_Europe

Para mayor información sobre los operadores celulares de los países del continente asiático (región del Océano Pacífico), consulte:

http://en.wikipedia.org/wiki/List_of_mobile_network_operators_of_the_Asia_Pacific_region

Para mayor información sobre los operadores celulares de los países del continente africano y del Oriente Medio, consulte:

http://en.wikipedia.org/wiki/List_of_mobile_network_operators_of_the_Middle_East_and_Africa

Recuerde que el kit del LNIntruder NO TRAE tarjeta SIM, y el Usuario Final debe adquirir una con su operador celular preferido. Para que la tarjeta SIM funcione en el LNIntruder, debe tener un plan de datos en prepago o postpago.

Antes de usar una tarjeta SIM en el LNIntruder, verifique que la navegación funciona desde un equipo de telefonía celular o desde un computador con un módem USB 3G.

Para introducir o cambiar la tarjeta SIM de su módem USB 3G ZTE MF190S, siga los pasos presentados a continuación:

Instalación Hardware

1. Ponga el dedo en la ranura de agarre inferior, y luego levante la cubierta frontal del módem para soltar y extraer.



Nota:

No abra la cubierta frontal bruscamente para evitar dañarla.

2. Inserte la tarjeta SIM/USIM en la ranura de la SIM/USIM. Inserte la tarjeta SIM/USIM con el área de contacto metálico hacia abajo en la ranura, y empuje la tarjeta SIM / USIM en la medida de lo posible, como se muestra en la siguiente imagen.



El manual de fabricante completo para el módem ZTE MF190S, en español, puede ser encontrado en:

http://www.zte.com.cn/endata/mobile/Spain/Spain_Instruction/201106/P020110616532363906332.pdf

Es importante tener en cuenta que el módem USB debe conectarse al LNIntruder **ANTES** de prenderlo, para que sea reconocido correctamente y éste inicie sus comunicaciones de manera normal.

14. CONSIDERACIONES FINALES

a. IPTables

El LNIntruder trae configuradas reglas de filtrado de paquetes (con IPTables), para prevenir su detección.

- El único tráfico TCP entrante permitido es el de los servicios SSH (puerto 22/tcp) y el de la Interfaz Web (puerto 10443/tcp), en todas sus interfaces de red. Todo el tráfico saliente del LNIntruder está permitido.
- El LNIntruder **NO** responde a paquetes ICMP ni UDP en ninguna interfaz de red (Por lo tanto, el LNIntruder **NO RESPONDE PING !!!**)
- Este filtrado de paquetes no interfiere para nada en la creación y mantenimiento de los túneles cifrados, pero podría intervenir en procesos de evaluación/ataque posteriores. De ser así, se recomienda eliminar las reglas de filtrado, removiendo el firewall, con el comando:

```
root@server:~# iptables -F
```

Este cambio es temporal, y las reglas de firewall volverán a levantarse automáticamente en el siguiente reinicio.

Si se requiere mantener un nivel de evasión elevado, y las reglas por defecto de filtrado de paquetes restringen el tráfico necesario, se recomienda diseñar un set de reglas de firewall apropiadas y remplazarlas.

b. Servidor LNIntruder MASTER

El servidor LNIntruder MASTER deberá estar en Internet y tener al menos un puerto TCP visible desde la red mundial. Si este servidor está detrás de un router o firewall, se deberá utilizar redireccionamiento de puertos (PAT – Port Address Translation) para que cuando en miniservidor LNIntruder intente comunicarse con la dirección IP válida y un puerto en particular, dicho tráfico le sea direccionado al servidor LNIntruder MASTER.

Para mayor información sobre PAT, te recomendamos leer:

http://es.wikipedia.org/wiki/Port_address_translation

http://en.wikipedia.org/wiki/Port_address_translation

15. BACKUP Y RESTAURACIÓN DEL LNINTRUDER

a. Backup Completo

- 1) Desconecte todos los periféricos que tenga conectados al LNIntruder (Módem USB 3G, tarjeta inalámbrica WiFi USB, Tarjeta SD, etc.) y reinicie su LNIntruder.
- 2) Conecte al puerto USB del LNIntruder un disco duro o llave USB de más de 4GB de tamaño.
- 3) Monte dicha unidad (i.e. /dev/sda1) en el sistema operativo del LNIntruder, por ejemplo, con los comandos:
root@server:~# mkdir /mnt/backup
root@server:~# mount -t auto /dev/sda1 /mnt/backup
- 4) Ingrese a un directorio dentro del disco montado y realice el backup:
root@server:~# cd /mnt/backup/
root@server:~# tar -zcpvf lnintruder-backup.tgz --exclude=/sys --exclude=/proc --exclude=/opt --exclude=/media --exclude=/mnt --exclude=/dev /
- 5) El backup completo tomará unos 8-12 minutos aproximadamente.
- 6) Cuando el backup termine, desmonte la unidad USB:
root@server:~# umount /mnt/backup

b. Restauración Completa

- 1) Desconecte todos los periféricos que tenga conectados al LNIntruder (Módem USB 3G, tarjeta inalámbrica WiFi USB, Tarjeta SD, etc.) y reinicie su LNIntruder.
- 2) Conecte al puerto USB del LNIntruder el medio de almacenamiento USB en que reside el backup.
- 3) Monte dicha unidad (i.e. /dev/sda1) en el sistema operativo del LNIntruder, por ejemplo, con los comandos:
root@server:~# mkdir /mnt/backup (SI NO ESTÁ CREADO)
root@server:~# mount -t auto /dev/sda1 /mnt/backup
- 4) Ingrese al directorio que contiene el backup y restáurelo:
root@server:~# cd /mnt/backup/
root@server:~# tar -zxpvf lnintruder-backup.tgz -C /
- 5) Cuando el proceso de restauración termine, desmonte la unidad USB y reinicie el miniservidor LNIntruder:
root@server:~# umount /mnt/backup
root@server:~# reboot