CAPÍTULO 4
CONFIGURACIÓN E IMPLEMENTACIÓN DE LAS HERRAMIENTAS DE DEFENSA

CONFIGURACIÓN E IMPLEMENTACIÓN DE LAS HERRAMIENTAS DE DEFENSA

En este capítulo se lleva a cabo la instalación y configuración de las herramientas de defensa para la red, se describe paso a paso el proceso de instalación y se hace una breve descripción de las configuraciones realizadas a cada herramienta y en qué área se va a implentar.

4.1 HERRAMIENTAS PARA REFORZAR EL SISTEMA OPERATIVO

4.1.1 *OpenSSH*

OpenSSH es una herramienta que se implementa en la mayoría de los sistemas operativos basados en Linux por lo que únicamente se mostrarán características básicas sobre su configuración.

El archivo de configuración del servidor se llama sshd_config y generalmente se encuentra en el directorio /etc/ssh. Para obtener un mejor rendimiento de SSH este archivo que se debe modificar.

Especificamos el protocolo a utilizar:

Protocol 2

Cambiamos el número de puerto estándar (22) por un puerto diferente (opcional):

Port 2220

No se permitirá el logueo del administrador directamente, ya que se puede cambiar de usuario una vez que se ingresa como usuario normal:

PermitRootLogin no

El número máximo de equivocaciones al ingresar el usuario y/o la contraseña se cambiará a dos:

MaxAuthTries 2

La cantidad de pantallas de login o cantidad de conexiones simultáneas de login que permitirá el sshd por ip se establecerá en 3:

MaxStartups 3

El servidor desconecta al cliente si no se ha logueado correctamente en 2 minutos:

LoginGraceTime 120

No usaremos el método de autenticación por rhosts:

RhostsAuthentication no

IgnoreRhosts yes

Establecemos que la conexión termine después de 3 minutos, para lo cual cada 60 segundos el servidor enviará un mensaje esperando respuesta del cliente, y el número de intentos para obtener respuesta será 3:

ClientAliveInterval 60

ClientAliveCountMax 3

No se permitirán passwords vacíos:

PermitEmptyPasswords no

4.1.2 BASTILLE LINUX

Para llevar a cabo el proceso correspondiente se debe abrir una interfaz de línea de comandos en la que se introducen los siguientes comandos:

yum install perl-Curses*

yum install perl-Tk*

tar jvxf Bastile-x-x.tar.bz2

cd Bastille

sh Install.sh

bastille –x

accept

bastille -x

Usaremos Bastille para aplicar actualizaciones para los agujeros de seguridad conocidos y para restringir y/o desactivar los servicios innecesarios en el sistema.

Al iniciar Bastille aparece la interfaz de configuración y una serie de preguntas con una explicación sobre cada área que se va a configurar, con una posible respuesta, SI o NO, como se muestra en la figura 4.1, Interfaz de configuración de Bastille.

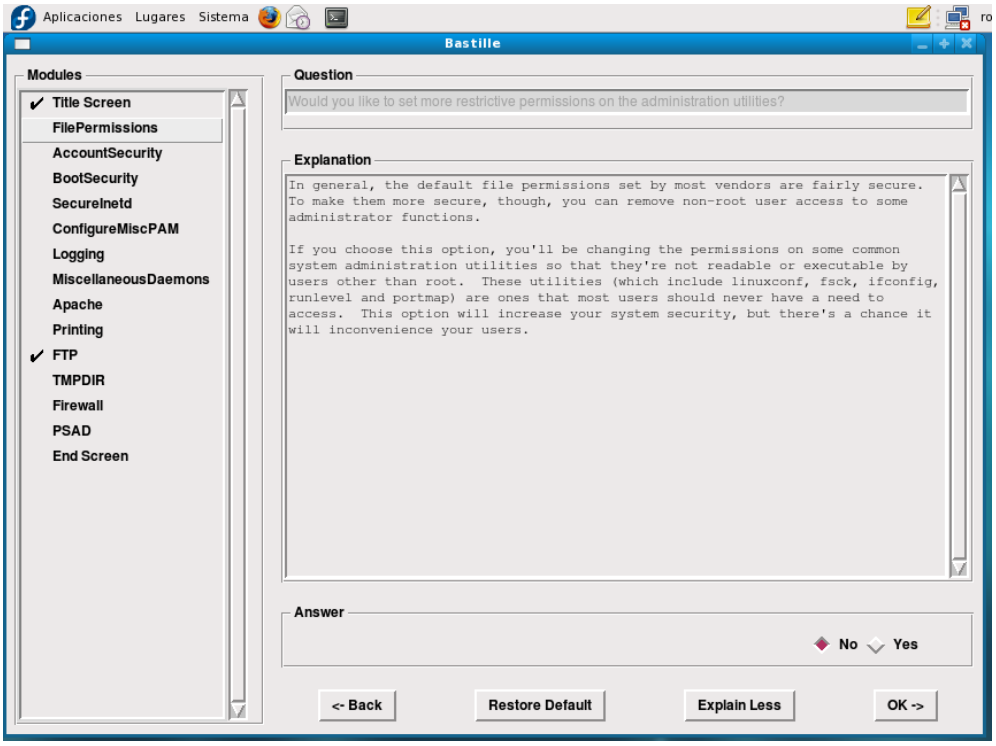


Figura 4.1, Interfaz de configuración de Bastille

- ***Would you like to set more restrictive permissions on the administration utilities? [N]***

  Útil en máquinas con múltiples cuentas de usuario pero en este caso se trata de una máquina dedicada para establecer el sistema de seguridad.

- ***Would you like to disable SUID status for mount/umount? [Y]***
- ***Would you like to disable SUID status for ping? [Y]***
- ***Would you like to disable SUID status for at? [Y]***

  Se deshabilitarán los programas SUID para evitar que usuarios sin privilegios ejecuten programas con permisos de administrador.

- ***Should Bastille disable clear-text r-protocols that use IP-based authentication? [Y]***

r-tools son un conjunto de utilidades para la administración remota de equipos que usan las direcciones *IP* como método de autenticación y no usan encriptación para el intercambio de información.

- ***Would you like to enforce password aging? [Y]***

  Se habilitará un tiempo de caducidad para las contraseñas, por default 180 días. Se deberá cambiar la contraseña antes de este plazo, de otra forma la cuenta será bloqueada.

- ***Would you like to restrict the use of cron to administrative accounts? [Y]***

  El uso de cron estará restringido sólo para la cuenta de administrador.

- ***Do you want to set the default umask? [Y]***

  El umask son los permisos por defecto que se le ponen a los archivos que se van creando.

- ***What umask would you like to set for users on the system? [077]***

  Continuación de la pregunta anterior, lo mejor es usar la opción 077 para que únicamente el dueño de los archivos pueda escribir o leer sobre ellos.

- ***Should we disallow root login on all ttys? [N]***

  Esta opción es extremadamente útil con equipos a los que se pueda acceder por SSH sin limitación en cuanto a la *IP* de origen. En este caso ya se limitó el acceso del administrador en el archivo de configuración de *OpenSSH*.

- ***Would you like to password-protect the GRUB prompt? [Y]***

  Si se tiene acceso físico al equipo cualquier persona podría reiniciar el equipo y obtener una consola de administrador pasándole ciertos parámetros al GRUB, por lo que se protegerá con una contraseña.

- ***Would you like to disable CTRL-ALT-DELETE rebooting? [N]***

  No se recomienda modificar este parámetro ya que si se tiene acceso físico al equipo también se puede tener un reinicio forzado del mismo.

- ***Would you like to password protect single-user mode? [Y]***

Este modo (mono-usuario) permite arrancar el sistema de manera que solamente puede acceder el administrador del equipo. Generalmente no solicita autenticación por lo que protegeremos este modo mediante una contraseña.

- ***Would you like to set a default-deny on TCP Wrappers and xinetd? [N]***

  Se permitirá que se ejecuten estos servicios de conectividad a internet.

- ***Should Bastille ensure the telnet service does not run on this system? [y]***

  Se desactivará el servicio telnet ya que es obsoleto y supone un riesgo grave de seguridad del sistema al transmitir datos sin cifrarlos.

- ***Should Bastille ensure inetd's FTP service does not run on this system? [y]***

  Lo mismo que telnet, ftp es un servicio inseguro, por lo que se deshabilitará.

- ***Would you like to display "Authorized Use" messages at log-in time? [N]***

  No se mostrará ningún mensaje al momento de loguearse. Esta opción se puede activar para mostrar un mensaje con las restricciones para uso del sistema.

- ***Would you like to disable the gcc compiler? [N]***

  Se mantendrá activo el compilador de C ya que podría usarse para desarrollo de aplicaciones o scripts.

- ***Would you like to put limits on system resource usage? [Y]***

  Con esta medida establecemos un límite de 150 procesos por usuario, suficiente para trabajar y evita un ataque por denegación de servicio.

AL DAR CLICK EN OK => System rosource limits have been set in the file /etc/security/limits.conf,which you can edit later as necessary.

- ***Should we restrict console access to a small group of user accounts? [N]***

  Permite denegar el acceso a la consola excepto a un grupo determinado de cuentas.

- ***Would you like to disable printing? [Y]***

  El dejar activo un servicio que no se utilizará supone un riesgo de seguridad.

- ***Would you like to run the packet filtering script? [N]***

Esta opción activaría el *firewall* nativo de Linux, en este caso no se activará porque posteriormente se implementa un *firewall* con la herramienta Turtle *Firewall*.

- ***Are you finished answering the questions, i.e. may we make the changes? [Y]***

  Respondemos afirmativamente para que se apliquen los cambios en el sistema.

Como se aprecia Bastille es una herramienta muy útil para el reforzamiento de un sistema operativo, que si bien no está muy actualizada, tiene como ventaja el poder realizar el reforzamiento de un sistema operativo tipo Linux de una manera sencilla y eficiente, con una interfaz intuitiva y esto permite conocer los puntos más importantes a reforzar en un sistema operativo.

4.2 PROTECCIÓN DE CONTRASEÑAS Y ATAQUES DE FUERZA BRUTA

4.2.1 John The Ripper

John the Ripper es una herramienta de mucha importancia para la administración de sistemas ya que nos permite encontrar de manera rápida y versátil las contraseñas débiles que se crean en el sistema.

Para la instalación de John the Ripper, únicamente se requiere el programa. A continuación se muestra la secuencia de comandos necesarios para realizar su instalación:

tar -zxvf john-1.7.5.tar.gz

cd john-1.7.5

cd src

make

make clean linux-x86-any

cd ../run

Ahora ya está instalado John the ripper, con la opción -- test se prueba el funcionamiento de dicho programa.

```
[root@localhost run]# ./john --test
Benchmarking: Traditional DES [24/32 4K]... DONE
Many salts:         77849 c/s real, 153852 c/s virtual
Only one salt:      61465 c/s real, 150650 c/s virtual
Benchmarking: BSDI DES (x725) [24/32 4K]... DONE
Many salts:         2785 c/s real, 5336 c/s virtual
Only one salt:      2798 c/s real, 5182 c/s virtual
```

```
Benchmarking: FreeBSD MD5 [32/32]... DONE
Raw:    2343 c/s real, 4922 c/s virtual
Benchmarking: OpenBSD Blowfish (x32) [32/32]... DONE
Raw:    145 c/s real, 382 c/s virtual
Benchmarking: Kerberos AFS DES [24/32 4K]... DONE
Short:  57958 c/s real, 139323 c/s virtual
Long:   181035 c/s real, 449900 c/s virtual
Benchmarking: LM DES [32/32 BS]... DONE
Raw:    1605K c/s real, 3536K c/s virtual
```

4.2.2 Cracklib

Cracklib es una biblioteca de comprobación de contraseñas y forma parte de la instalación predeterminada de las distribuciones Debian, Mandrake, RedHat y SuSE. Cracklib permite a los administradores de sistemas establecer reglas para la creación de contraseñas.

Para realizar la configuración se debe editar uno de los dos posibles archivos: /etc/pam.conf o /etc/pam.d/passwd

password required /lib/security/pam_cracklib.so minlen=10 dcredit=2 ocredit=2

password required /lib/security/pam_unix.so nullok use_authok md5

La primera columna de ambas instrucciones actualiza la información de autenticación, como cambiar la contraseña de un usuario, lo que le permite a dicho usuario el acceso al sistema de seguridad que controla las credenciales.

La siguiente columna determina el control de un servicio, o cómo debe administrarse su ejecución. El argumento “required” indica que si el servicio falla, las siguientes acciones se procesarán pero fallarán.

minlen=N, es la longitud mínima de la contraseña, igual a la cantidad de créditos, que deben obtenerse. Un crédito por unidad de longitud. La longitud rel de la nueva contraseña nunca puede ser menor que 6.

dcredit=N, indica la cantidad máxima de créditos por incluir dígitos (0-9).

ocredit=N, indica la cantidad máxima de créditos por incluir caracteres que no son letras ni números.

Use_authok se utiliza para apilar módulos en un servicio. En este caso, se añadió *md5* a la biblioteca pam_unix.so. Esto permite que las contraseñas se codifiquen con el algoritmo *MD5*.

4.3 SEGURIDAD DEL EQUIPO

4.3.1 Nessus

Para llevar a cabo la instalación de Nessus se recomienda seguir las indicaciones que se dan a continuación, en las cuales se presentan los comandos correspondientes y la respuesta del sistema sombreada para su fácil distinción:

Se descarga el archivo fuente de Nessus.
Se desempaqueta y descomprime el archivo, se ingresa al directorio y se ejecuta el archivo binario de instalación:

tar –zxvf Nessus-4.0.2.tar.gz
cd Nessus-4.0.2
./install.sh

```
This installation program will install or upgrade Nessus under /opt/nessus
Note that you're attempting to install the GENERIC version of Nessus 4
This setup is not supported in production. Try to use a specific RPM instead
```

Press [ENTER] to start the installation

[root@localhost Nessus-4.0.2]#
<enter>

```
.opt/nessus/var/nessus/nessus_org.pem
opt/nessus/var/nessus/users/
opt/nessus/var/nessus/nessus-services
opt/nessus/var/nessus/logs/
[Done]
 - Please run /opt/nessus/sbin/nessus-adduser to add a user
 - Register your Nessus scanner at http://www.nessus.org/register/ to obtain
   all the newest plugins
 - You can start nessusd by typing /sbin/service nessusd start
```

Se crea un usuario para Nessus:

[root@localhost Nessus-4.0.2]# /opt/nessus/sbin/nessus-adduser

```
Login : lsdpo
Authentication (pass/cert) : [pass]   <enter>lo dejamos en blanco
Login password : berliner&&
Login password (again) : berliner&&
Do you want this user to be a Nessus 'admin' user ? (can upload plugins, etc...) (y/n) [n]: y
User rules
----------
nessusd has a rules system which allows you to restrict the hosts that nessus_user has the right to test. For
instance, you may want him to be able to scan his own host only.
Please see the nessus-adduser manual for the rules syntax
Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)
```

```
Login           : lsdpo
Password        : ***********
This user will have 'admin' privileges within the Nessus server
Rules           :
Is that ok ? (y/n) [y]
User added
```

Ahora registramos el código de activación para usar los plugins de Nessus.
[root@localhost Nessus-4.0.2]# /opt/nessus/bin/nessus-fetch --register 475F-7F48-7D5B-240D-B222

```
Your activation code has been registered properly - thank you.
Now fetching the newest plugin set from plugins.nessus.org...
Your Nessus installation is now up-to-date.
If auto_update is set to 'yes' in nessusd.conf, Nessus will

update the plugins by itself.
```

Se debe crear ahora un certificado SSL para el servidor:
[root@localhost Nessus-4.0.2]# /opt/nessus/sbin/nessus-mkcert

```
-------------------------------------------------------------------------------
                        Creation of the Nessus SSL Certificate
-------------------------------------------------------------------------------
This script will now ask you the relevant information to create the SSL
certificate of Nessus. Note that this information will *NOT* be sent to
anybody (everything stays local), but anyone with the ability to connect to your
Nessus daemon will be able to retrieve this information.
CA certificate life time in days [1460]:
Server certificate life time in days [365]:
Your country (two letter code) [FR]: MX
Your state or province name [none]: DF
Your location (e.g. town) [Paris]: DF
Your organization [Nessus Users United]: UNAM
Congratulations. Your server certificate was properly created.
The following files were created :
Certification authority :
Certificate = /opt/nessus/com/nessus/CA/cacert.pem
 Private key = /opt/nessus/var/nessus/CA/cakey.pem
 Nessus Server :
 Certificate = /opt/nessus//com/nessus/CA/servercert.pem
 Private key = /opt/nessus//var/nessus/CA/serverkey.pem
```

Para que el servidor comience a usar los nuevos certificados, se deberán agregar al archivo de configuración (nessusd.conf) las siguientes líneas y luego reiniciar el servidor:

```
 echo "cert_file=/opt/nessus//com/nessus/CA/servercert.pem" >>
/opt/nessus/etc/nessus/nessusd.conf

echo "key_file=/opt/nessus//com/nessus/CA/serverkey.pem" >>
/opt/nessus/etc/nessus/nessusd.conf
```

echo "ca_file=/opt/nessus//com/nessus/CA/cacert.pem" >>
/opt/nessus/etc/nessus/nessusd.conf

echo "#force_pubkey_auth = yes" >> /opt/nessus/etc/nessus/nessusd.conf

La última línea (#force_pubkey_auth = yes) es una configuración que le indica al servidor que para permitir que cualquier usuario se conecte, deberá presentar sus certificados. En el último comando estamos pasando esa configuración pero de forma comentada (no se utilizará) lo que significa que los usuarios podrán conectarse al servidor de Nessus usando su clave normal sin necesidad de usar certificados, si se descomenta esa opción, los usuarios no solo deberán presentar su clave sino que también tendrán que usar sus certificados para que Nessus lo pueda autorizar.

Parar Nessus:

/sbin/service nessusd stop

killall nessus-service

Reiniciar Nessus para que cargue los plugins:
/opt/nessus/sbin/nessus-service -D

Ahora se crea el certificado del cliente:
[root@localhost Nessus-4.0.2]# /opt/nessus/sbin/nessus-mkcert-client

Do you want to register the users in the Nessus server as soon as you create their certificates ? [n]: y

-[root@Kakaroto software]# /opt/nessus/sbin/nessus-mkcert-client

Do you want to register the users in the Nessus server

as soon as you create their certificates ? [n]: y

Creation Nessus SSL client Certificate

This script will now ask you the relevant information to create the SSL
client certificates for Nessus.
Client certificate life time in days [365]:
Your country (two letter code) [FR]: MX
Your state or province name []: DF

Your location (e.g. town) [Paris]: DF
Your organization []: UNAM
Your organizational unit []: ING
****
We are going to ask you some question for each client certificate
If some question have a default answer, you can force an empty answer by

```
entering a single dot '.'
**********
User #1 name (e.g. Nessus username) []: lsdpo
User lsdpo already exist
Do you want to go on and overwite the credentials?  [y]: y^C
[root@Kakaroto software]# /opt/nessus/sbin/nessus-mkcert-client
Do you want to register the users in the Nessus server
as soon as you create their certificates ? [n]: y
-------------------------------------------------------------------------------
                        Creation Nessus SSL client Certificate
-------------------------------------------------------------------------------
This script will now ask you the relevant information to create the SSL
client certificates for Nessus.
Client certificate life time in days [365]:
Your country (two letter code) [FR]: MX
Your state or province name []: DF
Your location (e.g. town) [Paris]: DF
Your organization []: UNAM
Your organizational unit []: ING
**********
We are going to ask you some question for each client certificate
If some question have a default answer, you can force an empty answer by
entering a single dot '.'
**********
User #1 name (e.g. Nessus username) []: lsdpo
User lsdpo already exist
Do you want to go on and overwite the credentials?  [y]: y
Should this user be administrator?  [n]: y
Country (two letter code) [MX]:
State or province name [DF]:
Location (e.g. town) [DF]:
Organization [UNAM]:
Organizational unit [ING]:
e-mail []: lsdpo@yahoo.com.mx
User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that $login has the right to test. For instance, you may want
him to be able to scan his own host only.
Please see the nessus-adduser(8) man page for the rules syntax
Enter the rules for this user, and enter a BLANK LINE once you are done:
(the user can have an empty rules set)
User added to Nessus.
Another client certificate?  [n]: n
Your client certificates are in /tmp/nessus-136e615c

You will have to copy them by hand
```

[root@localhost Nessus-4.0.2]# cp /tmp/nessus-136e615c/* /usr/local/software/certs/

Archivos creados

```
Certification authority :
/opt/nessus/com/nessus/CA/cacert.pem
/opt/nessus/var/nessus/CA/cakey.pem
Nessus Server :
 /opt/nessus/com/nessus/CA/servercert.pem
/opt/nessus/var/nessus/CA/serverkey.pem
```

Iniciar Nessus:

/opt/nessus/sbin/nessus-service -D

Para concluir el proceso Nessus:
killall nessus-service

Actualizamos los plugins:
/opt/nessus/sbin/nessus-update-plugins

Ahora se hace la instalación y configuración del cliente de Nessus:

cd /usr/local/software

rpm -Uvh NessusClient-4.0.2-fc10.i386.rpm

Se lanza el cliente de Nessus (figura 4.2, Cliente de Nessus).

/opt/nessus/bin/NessusClient

Figura 4.2, Cliente de Nessus

En esta parte se configura la conexión a través de SSL y mediante los certificados que creamos anteriormente, se hace click en Connect... y se abre la ventana de edición de la conexión.

El nombre de la conexión sirve para identificar dicha conexión. Host name puede ser el nombre del host o su dirección *IP*, por ejemplo "localhost". El login y el password deben ser las credenciales del servidor Nessus.

Una alternativa a la autenticación basada en credenciales es el uso del certificado SSL. Esto se configura haciendo click en el botón SSL Setup y proporcionando las rutas a los archivos cacert.pem, cakey.pem y servercert.pem como se muestra en la figura 4.3, Certificado SSL.

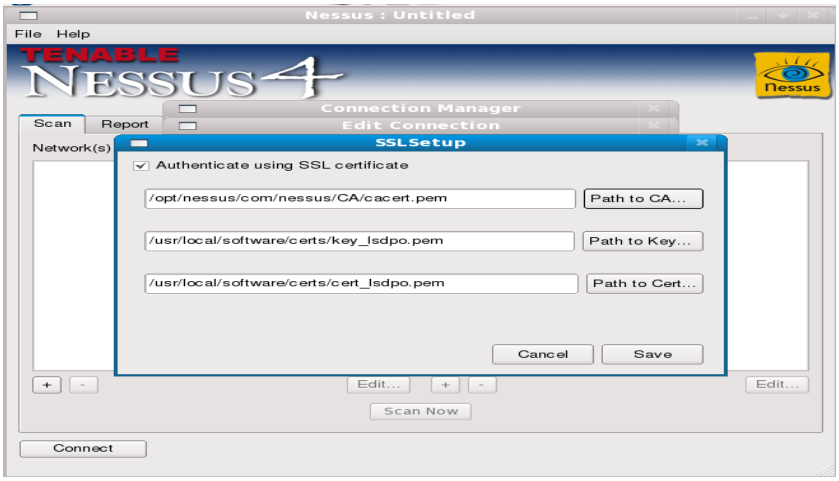


Figura 4.3 Certificado SSL.

Ahora ya se realizó la conexión entre el cliente y el servidor de Nessus y se pueden agregar políticas de escaneo a la medida haciendo click en el signo "+"(figura 4.4, Políticas de escaneo).

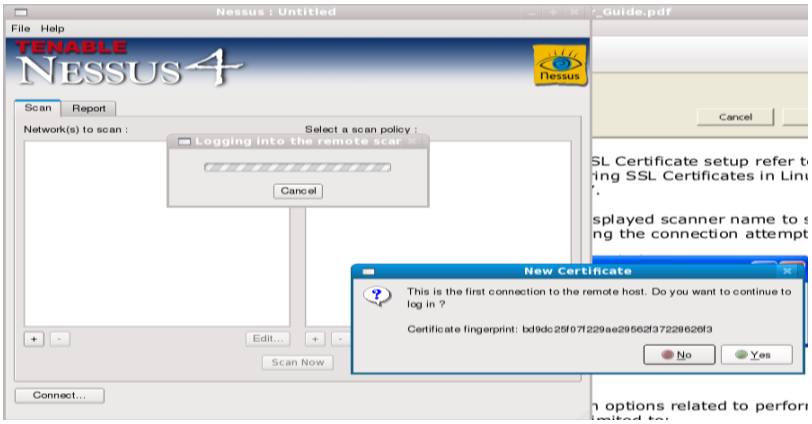


Figura 4.4, Políticas de escaneo.

4.4 HERRAMIENTAS PARA WEB

4.4.1 Nikto

Nikto se basa en la biblioteca LibWhisker, es una herramienta compatible con Capa de conexión segura (SSL), proxies y rastreos de puertos. Debido a que Nikto es un rastreador basado en *Perl*, funciona en Unix, Windows y Mac OS X.

Para llevar a cabo el proceso de instalación de la herramienta Nikto se requieren *OpenSSL* y *Apache*, por lo que después de hacer la descarga de dichos programas se ejecutan los siguientes comandos para hacer su instalación.

Instalación de *OpenSSL*:

```
tar -zxvf cd openssl-0.9.8e
cd openssl-0.9.8e
./config --prefix=/usr/local/ssl
make
make install
```

Instalación de *Apache*:

```
tar -zxvf httpd-2.0.61.tar.gz
cd httpd-2.0.61
./configure --prefix=/usr/local/apache2 --enable-so --enable-ssl --with-ssl=/usr/local/ssl
make
make install
```

Se inicia *Apache* con:
/usr/local/apache2/bin/apachectl start
Se detiene apache con
/usr/local/apache2/bin/apachectl stop

Ahora se desempaqueta y descomprime Nikto:
tar -zxvf nikto-2.1.0.tar.gz
cd nikto-2.1.0

Ya se puede ejecutar Nikto desde la línea de comandos para realizar un escaneo de los servicios web:

```
perl nikto.pl -h localhost:8080
```

4.5 RASTREADORES

Al proceso de escoger un lugar dentro de la red para ubicar ahí el sniffer generalmente es conocido por los analistas como "tapping the network" o "tapping into the wire", literalmente se traduce como "escuchar la red"[19]. Esto es esencial ya que va a determinar el alcance de la "escucha" del sniffer.

Escuchando en un entorno de hubs

Cuando se tiene una red con hubs instalados, simplemente se tiene que conectar el sniffer en un puerto disponible del hub. Esto es el sueño de todo analista de paquetes ya que un entorno así facilita mucho la tarea de hacer la escucha en la red. Como se sabe, el tráfico enviado a través de un hub es también enviado a todos los puertos conectados a dicho hub.

Aun así, es raro encontrar una red que utilice hubs. Los hubs alentan mucho el tráfico en la red, ya que solo un dispositivo a la vez puede hacer uso del hub, por ello los dispositivos tienen que competir entre si por el ancho de banda. Cuando dos dispositivos se comunican al mismo tiempo hay una colisión de paquetes, éstos se pierden y tiene que ser retransmitidos.
En esta situación, por lo único que se tiene que preocupar el analista de paquetes es por el volumen de tráfico de la captura, ya que se captura todo el tráfico que va de y hacia los dispositivos conectados al hub y esto puede generar una gran cantidad de datos, muchos de ellos irrelevantes.

Escucha en un entorno con switches

Este tipo de entorno es más común, como se sabe, el switch tiene la ventaja de transmitir datos a través de tráfico broadcast, unicast y multicast. También permiten hacer una transmisión full dúplex, esto es, se puede transmitir y recibir información de forma simultánea. Esto supone una gran ventaja para la red pero agrega complejidad a la escucha de la misma, ya que el único tráfico que se puede ver cuando se conecta un sniffer a un puerto libre del switch, es el tráfico broadcast y el tráfico enviado y recibido por la propia máquina en la que se encuentra instalado el sniffer.

Hay tres formas de hacer una escucha en un dispositivo conectado a un switch:

Port mirroring (copia de puerto), envenenamiento de ARP y hubbing out.

Port mirroring

Este es quizá el modo más sencillo de escuchar en la red un dispositivo en particular. Se requiere un switch que permita la copia de puertos. A su vez se requiere el acceso a la interfaz de línea de comandos del switch para habilitar esta característica. Si se requiere,

por ejemplo, hacer la escucha de un dispositivo conectado al puerto 3, se conecta el sniffer en el puerto 4 y se habilita al switch para que copie al puerto 4, todo el tráfico que pasa por el puerto 3.

Hubbing out

En caso de que el switch no soporte port mirroring, lo que se hace habitualmente es conectar un hub entre el dispositivo objetivo y el switch y conectar el sniffer a dicho hub, con lo que el dispositivo objetivo y el sniffer se encontrarían en mismo dominio de broadcast. Esto no se considera una práctica muy "limpia", ya que reduce el tráfico de full dúplex a half dúplex, pero se considera una buena alternativa cuando el switch no permite la copia de puertos.

Envenenamiento de ARP

El envenenamiento de ARP o ARP spoofing es el proceso mediante el cual se envían mensajes ARP a un switch o router con una dirección MAC falsa para interceptar o detener tráfico de algún dispositivo conectado. Esta técnica requiere de herramientas como Cain & Abel para ser implementada en una red y se debe ser muy cuidadoso pues puede saturar la computadora a la que se redirecciona el tráfico creando problemas de rendimiento en la red y cuellos de botella.

Escucha en un medio con routers

Cuando se requiere hacer la escucha en redes con uno o varios routers para solucionar algún problema de la red, se debe estar consciente del alcance de cada segmento de la red. Como se sabe, un dominio de broadcast se extiende hasta que alcanza un router, por ello es importante definir en que segmento se va a hacer la escucha. Para este propósito son muy importantes los mapas o diagramas de red, ya que permiten definir una mejor ubicación del sniffer, donde se pueda sacar el mejor provecho.

4.5.1 Wireshark

Para realizar la instalación correspondiente a esta herramienta es necesario realizar las siguientes actividades:

Wireshark requiere varias dependencias para la creación de la interfaz gráfica, éstas son:
glib, atk, gtk, pango y cairo:
yum install glib
yum install pango
yum install cairo

yum install atk
yum install gtk+
Ahora se instala la dependencia libpcap para la captura de datos:
cd libpcap-1.0.0
./configure
make
make install

Finalmente se instala Wireshark:
tar –jvxf wireshark-1.4.1.tar.bz2
cd wireshark-1.4.1
./configure
make
make install

Para iniciar Wireshark con su interfaz gráfica solamente se ejecuta el comando "wireshark".

4.6 HERRAMIENTAS PARA AUDITAR Y DEFENDER LA RED

4.6.1 Turtle *Firewall*

Turtle *Firewall* es un conjunto de secuencias de comandos *Perl* que hacen todo el trabajo de configurar un *firewall* Iptables automáticamente. Este programa facilita la observación de las reglas para estar seguros de obtener las declaraciones en el orden correcto.

Para la instalación de Turtle *Firewall* requerimos de una herramienta llamada Webmin. Esta herramienta permite hacer la configuración de un sistema por medio de la web y controlar y modificar aplicaciones como *Apache*, Mysql, PHP y *DHCP*, entre otras.

Se descarga el archivo rpm y lo instalamos:
rpm -Uvh webmin-1.500-1.noarch.rpm

```
advertencia:webmin-1.500-1.noarch.rpm: CabeceraV3 DSA signature: NOKEY, key ID 11f63c51
Preparando...                ########################################### [100%]
Operating system is Redhat Linux
   1:webmin                  ########################################### [100%]
Webmin install complete. You can now login to http://localhost.localdomain:10000/
as root with your root password.
```

Ahora se inicia el servidor *Apache*:
/usr/local/apache2/bin/apachectl start

Y en un navegador se ingresa el URL http://localhost.localdomain:10000/ y aparecerá la ventana para autenticarse y establecer una contraseña, el nombre de usuario debe ser un nombre de usuario administrador del sistema, al igual que la contraseña, figura 4.5, Interfaz Webmin y finalmente la interfaz de configuración de Webmin, figura 4.6.

Figura 4.5, Interfaz Webmin.

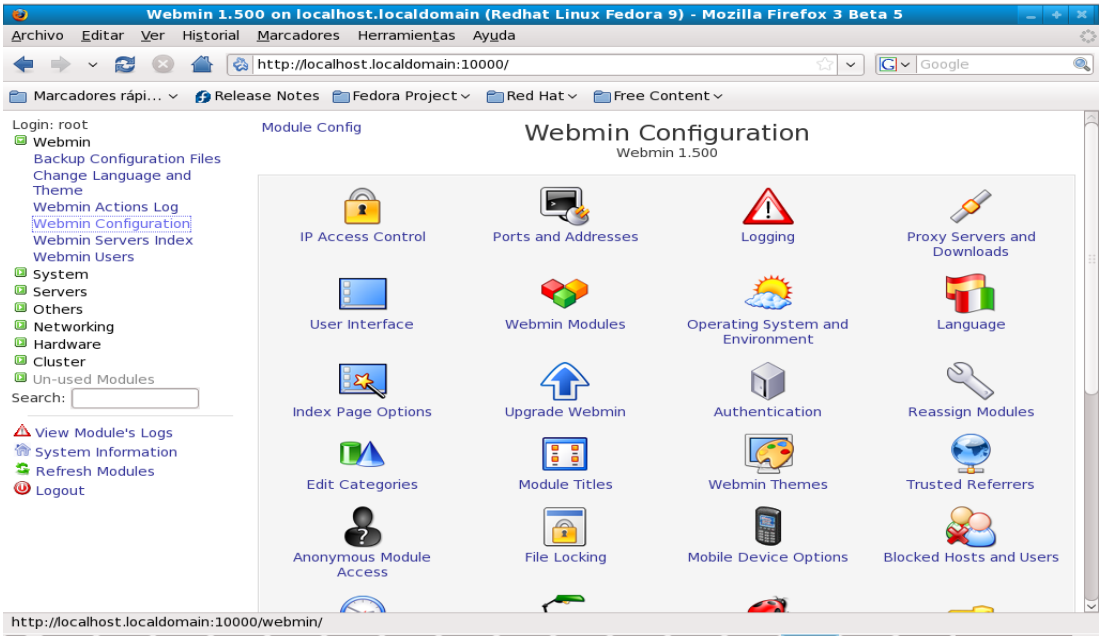


Figura 4.6, Interfaz de configuración de Webmin

Ahora se descarga el archivo de Turtle *Firewall* y se descomprime:

gzip -d turtlefirewall-1.37.wbm.gz

En el navegador nos dirigimos al link “configuration” y después al link “webmin modules”, en install module elegir “from uploaded file” y darle la ruta completa al archivo turtlefirewall-1.37.wbm, figura 4.7, Módulos Webmin.

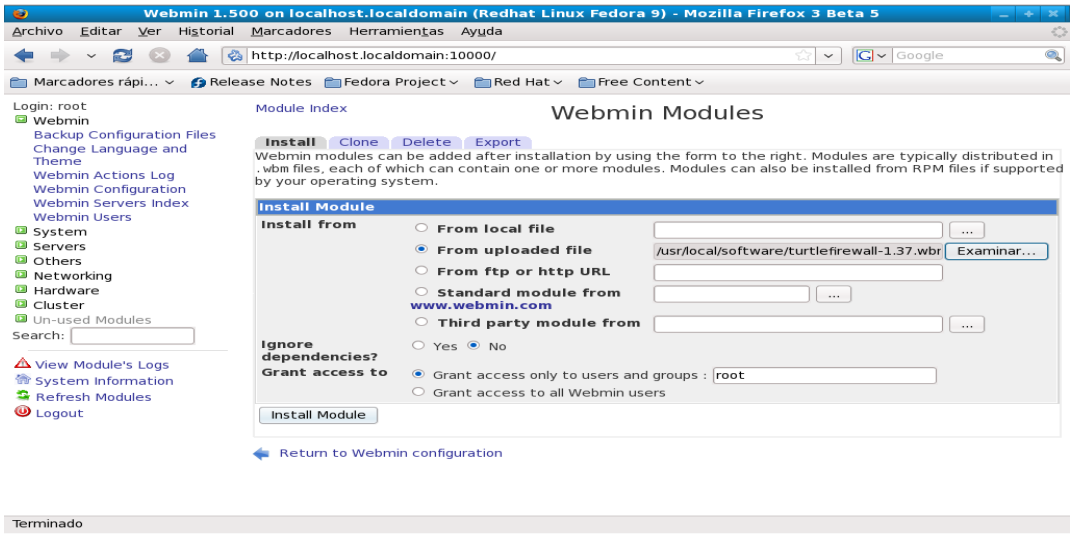


Figura 4.7, Módulos Webmin

Se hace click en instalar los scripts de inicio de Turtle *Firewall* y aparece la ventana de configuración de las reglas de Turtle *Firewall*, figura 4.8, Turtle *Firewall*.

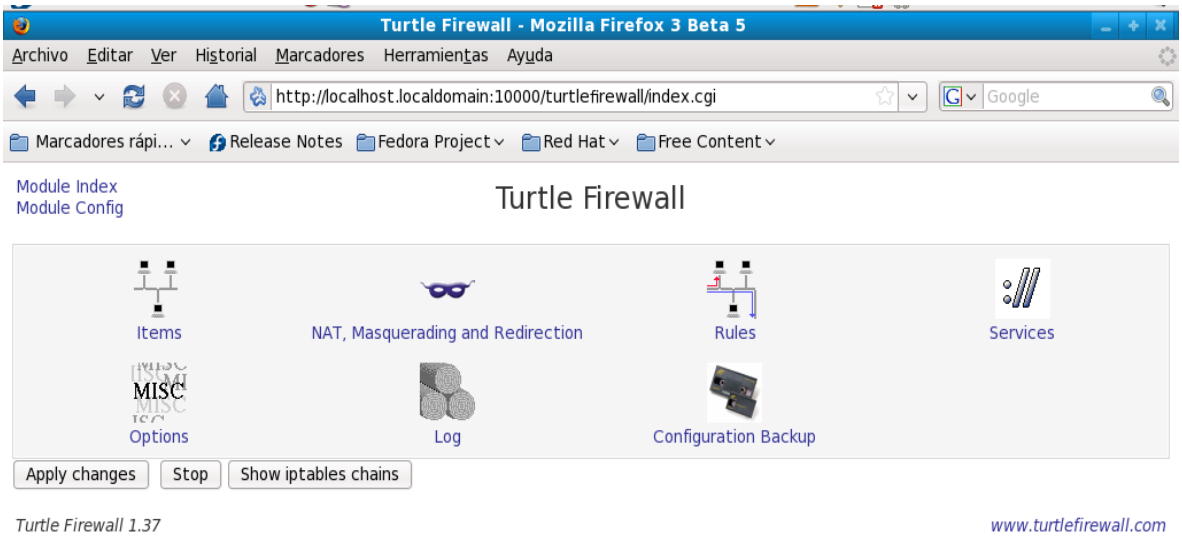


Figura 4.8, Turtle *Firewall*

4.6.2 BASE

BASE (Basic Analysis and Security Engine), el Motor de Seguridad de Análisis Básico, es una aplicación basada en ACID (Analysis Console for Intrusion Databases) la consola de análisis para bases de datos de intrusión.

Antes de instalar BASE se requiere tener instalada una base de datos y php, A continuación se describe paso a paso el proceso de instalación.

OpenSSL

Bajar openssl-0.9.8e.tar.gz
tar -zxvf openssl-0.9.8e.tar.gz
cd openssl-0.9.8e
./config --prefix=/usr/local/ssl
make
make install
Apache
tar -zxvf httpd-2.0.63.tar.gz
cd httpd-2.0.63
./configure --prefix=/usr/local/apache2 --enable-so --enable-ssl --with-ssl=/usr/local/ssl
make
make install
/usr/local/apache2/bin/apachectl start
 /usr/local/apache2/bin/apachectl stop

Librerías

libpng es una librería del formato de imágenes PNG, es dependiente de zlib.

tar -zxvf libpng-1.2.23.tar.gz
cd libpng-1.2.23
make prefix=/usr ZLIBINC=/usr/include ZLIBLIB=/usr/lib -f scripts/makefile.linux
make -f scripts/makefile.linux test
make prefix=/usr install -f scripts/makefile.linux

Librería grafica GD
tar -zxvf gd-2.0.33.tar.gz
cd gd-2.0.33
./configure --prefix=/usr/local/gd
make
make install

Libpcap es una librería para la captura de paquetes.
tar -zxvf libpcap-1.0.0.tar.gz
cd libpcap-1.0.0
./configure
make
make install

Readline le permite a los usuarios editar líneas de comando, esto facilita usar las teclas de flechas para insertar caracteres o desplazarse a través del historial de comandos.
tar -zxvf readline-5.2.tar.gz
cd readline-5.2
./configure
make
make install

Libxml2 es una librería de "parsing" xml para el lenguaje C, desarrollada por el proyecto Gnome.
tar -zxvf libxml2-2.6.29.tar.gz
cd libxml2-2.6.29
./configure
make
make install

Zlib es una biblioteca de compresión de datos que provee una implementación del algoritmo Deflate usado en el programa de compresión gzip.
tar -zxvf zlib-1.2.3.tar.gz
cd zlib
cd 1.2.3
./configure
make
make install
Jpeg es una librería que permite la compresión de archivos de imagen basándose en el estándar del Joint Photographic Experts Group.
tar -zxvf jpeg-6b.tar.gz
cd jpeg/src
./configure
make
make install
o en su caso rpm -Uvh libjpeg-devel-6b-26.i386.rpm

Instalación de la base de datos Mysql
groupadd mysql
useradd -g mysql mysql

```
tar -zxvf mysql-5.1.46.tar.gz
cd  mysql-5.1.46
./configure --prefix=/usr/local/mysql
make
make install
cp support-files/my-medium.cnf /etc/my.cnf
cp: ¿sobreescribir «/etc/my.cnf»? (s/n) s
cd /usr/local/mysql
chown -R mysql .
chgrp -R mysql .
.bin/mysql_install_db --user=mysql
chown -R root .
chown -R mysql var
.bin/mysqld_safe --user=mysql &

su – mysql
cd /usr/local/mysql/bin
./mysql -u root
mysql>show databases;
mysql>exit
exit
y como usuario root

para detener mysql:

/usr/local/mysql/bin/mysqladmin shutdown

 ./mysqladmin -u root password "my5q1&"

Después como usuario mysql podemos iniciar la base con
/usr/local/mysql/bin/mysqld_safe --user=mysql &
cd /usr/local/mysql/bin
y pararlo:
./mysqladmin -u root shutdown –p

Se establece un password para mysql
mysql -u root mysql
mysql>update user set password=PASSWORD('my5q1&') where user='root'
;
Query OK, 3 rows affected (0,00 sec)
Rows matched: 3  Changed: 3  Warnings: 0
mysql>flush privileges;

Ahora nos ingresamos con:
```

./mysql -u root -p
y el password

Instalación de PHP
tar -zxvf php php-5.3.2.tar.gz
cd php-5.3.2
./configure --prefix=/usr/local/php --with-apxs2=/usr/local/apache2/bin/apxs --with-config-file-path=/usr/local/php --enable-sockets --with-mysql=/usr/local/mysql --with-zlib-dir=/usr/local --with-gd=/usr/local/gd --with-png-dir=/usr/include/libpng12 --with-jpeg-dir=/usr/local/jpeg
make
make install
ahora se configura php
cp php.ini-dist/usr/local/php/php.ini
en el caso de php 5.3.2
cp php.ini-production /usr/local/php/php.ini

Se modifica el archivo httpd.conf

vi /usr/local/apache2/conf/httpd.conf
DirectoryIndex index.html
queda:
DirectoryIndex index.html index.html.var index.php

Y finalmente se agregan las siguientes lineas:

AddType application/x-httpd-php .php .php4 .php5 .phtml .html
AddType application/x-httpd.php-source .phps
AddType image/x-icon .ico

Instalación de Snort
Instalación de libpcap 1.0.0
tar –zxvf libpcap-1.0.0.tar.gz
cd libpcap-1.0.0
./configure
make
make install

Instalación de pcre
tar -zxvf pcre-8.02.tar.gz
cd pcre-8.02
./configure

make
make install

Instalación de libnet
tar -zxvf libnet-1.0.2a.tar.gz
cd Libnet-1.0.2a/
En caso de ser necesario, también se instalan flex y bison.

./configure&&make&&make install

tar -zxvf snort-2.8.5.2.tar.gz
cd snort-2.8.5.2
./configure --enable-targetbased &&make&&make install
mkdir /etc/snort
mkdir /var/log/snort
cd /etc/snort
se copia el archivo snortrules-snapshot a /etc/snort
tar -zxvf snortrules-snapshot-2.8.tar.gz
cp etc/* /etc/snort
ln -s /usr/local/bin/snort /usr/sbin/snort
groupadd snort
useradd -g snort snort
chown snort:snort /var/log/snort
touch /var/log/snort/alert
chown snort:snort /var/log/snort/alert
chmod 600 /var/log/snort/alert
cp /etc/snort/so_rules/precompiled/FC-9/i386/2.8.4/*.so /usr/local/lib/snort_dynamicrules
mv /usr/local/lib/snort_dynamicrules /usr/local/lib/snort_dynamicrule

cp snort.conf /etc/snort/
cp: ¿sobreescribir «/etc/snort/snort.conf»? (s/n) s

Editamos el archivo /etc/snort

vi /etc/snort/snort.conf
Cambiamos la variable RULE_PATH por /etc/snort/rules
Comentamos las líneas con la frase output modules on.
Localizamos la frase "output log_unified". Debajo de esta línea insertamos lo siguiente:
output unified2: filename snort.log, limit=128

Probamos snort
[root@localhost snort]# snort -c /etc/snort/ -T

```
        --== Initialization Complete ==--
   ,,_     -*> Snort! <*-
  o"  )~   Version 2.8.5.2 (Build 121)
```

```
   ""    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team
         Copyright (C) 1998-2009 Sourcefire, Inc., et al.
         Using PCRE version: 8.01 2010-01-19
Snort successfully loaded all rules and checked all rule chains!
Snort exiting
```

Se levanta la base de datos
su – mysql
cd /usr/local/mysql/bin/

levantamos la base de datos
./mysqld_safe --user=mysql &
./mysql --user=root -p

Si aun no tiene password mysql se lo creamos
mysql> UPDATE user SET Password=PASSWORD('my5q1&') WHERE user='root';

password de mysql my5q1&

Ahora como usuario root creamos la base de datos snort

mysql>create database snort;
y le asignamos un password a snort
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.*to
snort@localhost;
SET PASSWORD FOR snort@localhost=PASSWORD('5n0rt&');
exit

Se crea las tablas de snort
cd /usr/local/mysql/bin/
./mysql --user=root -p < /usr/local/software/snort-2.8.5.2/schemas/create_mysql snort
y se verifica que se hayan creado las tablas correctamente

mysql -p
SHOW DATABASES; Debe haber 4 bases de datos
use snort
SHOW TABLES; Debe haber 16 tablas
exit
exit
ahora como usuario root

Instalación de BASE y ADODB

cd /var/www/html
 cp /root/Escritorio/snort/adodb511.tgz .
 cp /root/Escritorio/snort/base-1.4.5.tar.gz .
 tar zxvf adodb511.tgz

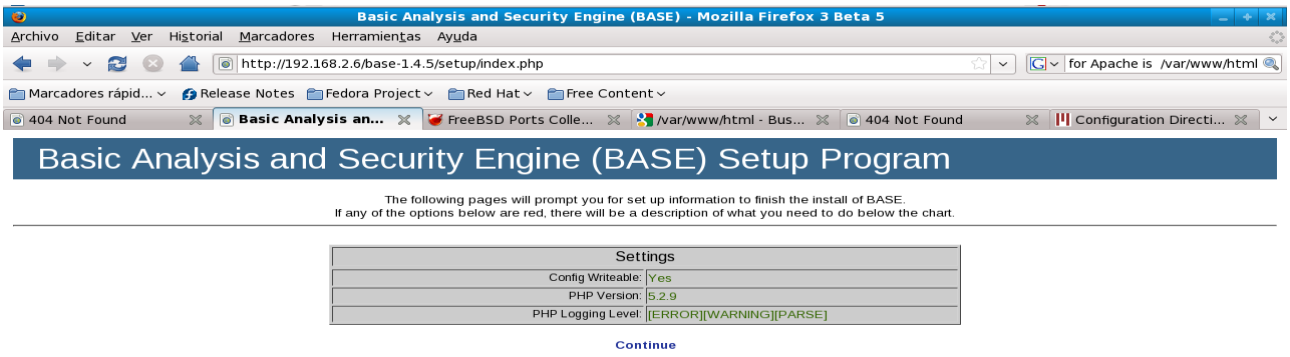
tar -zxvf base-1.4.5.tar.gz
chown apache base-1.4.5
chgrp apache base-1.4.5
chmod 777 /var/www/html/base-1.4.5
vi /etc/php.ini

Verificamos que la variable error reporting tenga el siguiente parámetro:

error_reporting = E_ALL & ~E_NOTICE
Instalamos mail y mail_mime, dos funciones de php que se requieren para la interfaz gráfica.
cd /usr/local/php/bin
y ejecutamos
./pear install Mail
./pear install Mail_Mime

Ahora se reinicia el servicio.
service httpd restart
El servidor debe estar configurado para que lea /var/www/html
en el archivo /usr/local/apache/conf/httpd.conf
#DocumentRoot "/usr/local/apache2/htdocs"

DocumetRoot "/var/www/html"
Ahora se abre un navegador y se ingresa la siguiente dirección:
http://localhost/base-1.4.5/setup/index.php
La salida se muestra en la figura 4.9, Instalacion de BASE 1.



4.9 Instalación de BASE 1

click en continue

Ingresamos la ruta a adodb /var/www/html/adodb5, figura 4.10, Ruta a Adodb.

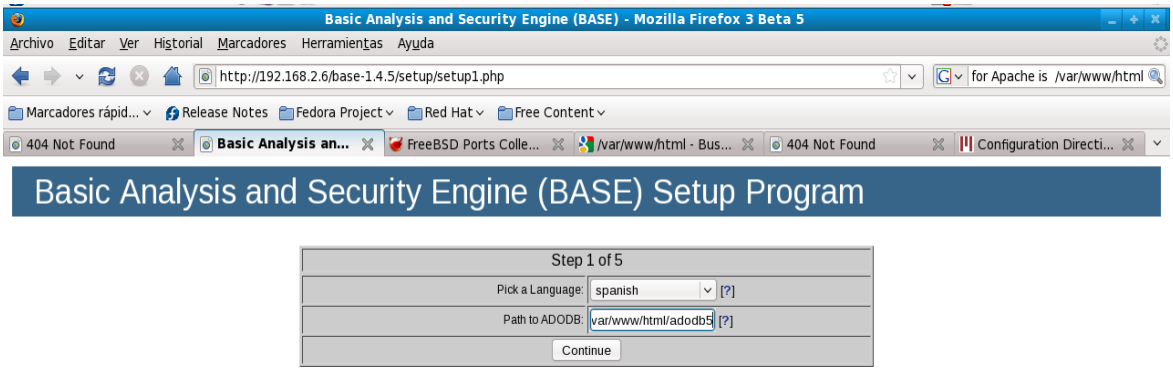


Figura 4.10, Ruta a Adodb

Ahora se ingresan los parámetros del usuario snort en la base de datos. Figura 4.11, Parámetros de Snort.
Database Name=snort, Database Host=localhost, Database User=snort, Database Password=5n0rt&

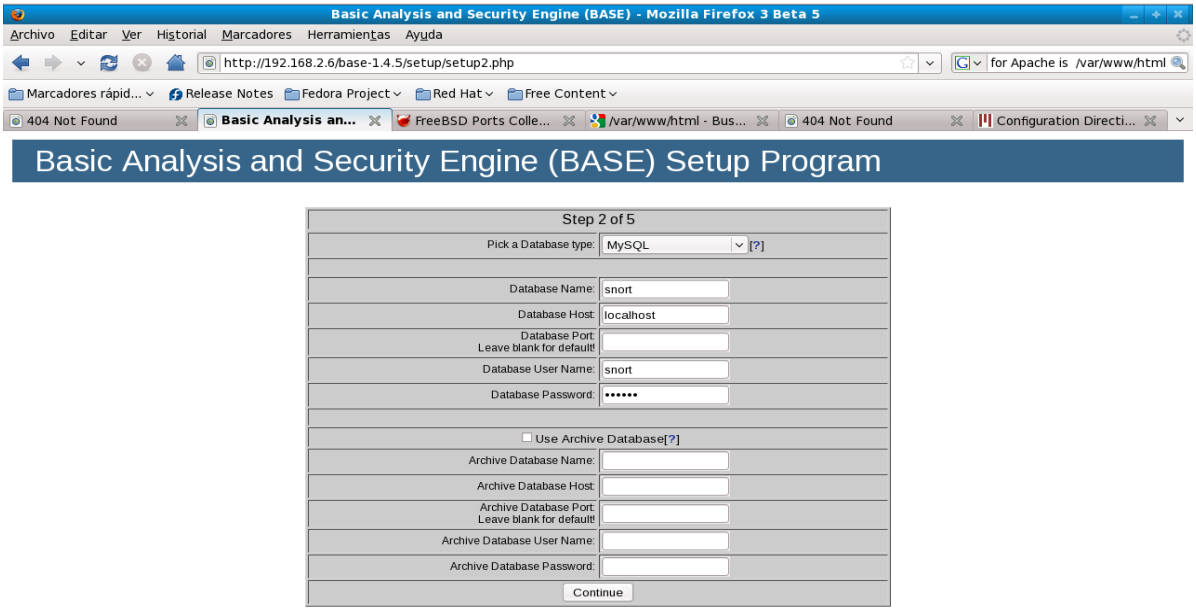


Figura 4.11, Parámetros de Snort

En la siguiente pantalla se ingresa el nombre de usuario del administrador de Snort así como su password.
Admin User Name=snort, Password=5n0rt&, Full Name=snort

El siguiente paso es hacer click en Create BASE AG para agregar las tablas en la base de datos de Snort que dan soporte a BASE. Figura 4.12, Create BASE AG.

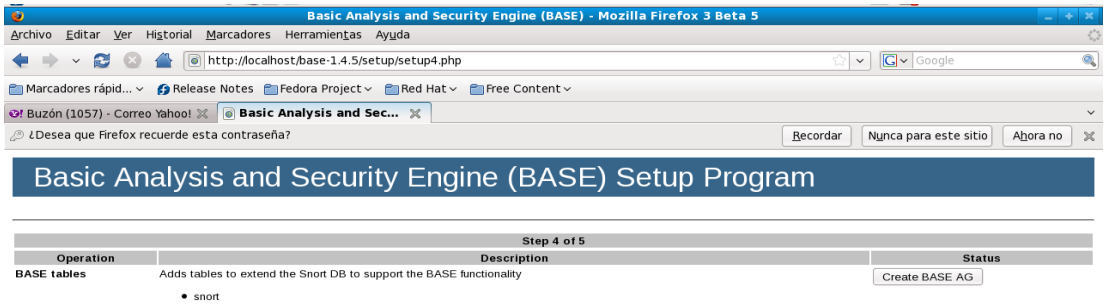


Figura 4.12, Create BASE AG.

Después se hace click en "ir al paso 5" y aparece lo siguiente, Figura 4.13, Instalación final BASE:

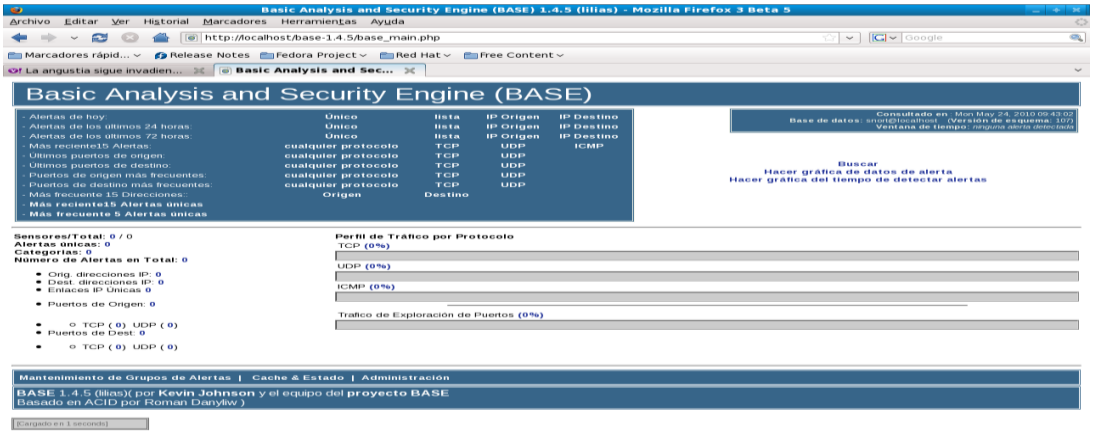


Figura 4.13 Instalación final BASE

Instalación de Barnyard

Barnyard es un intérprete de información de las bitácoras de Snort a MYSQL, su instalación se realiza de la siguiente manera:

tar -zxvf barnyard2-1.8.tar.gz
Primero se debe detener mysql porque cuando está levantado no se pueden leer sus archivos y es necesario leerlos para la instalacion de barnyard.
cd barnyard2-1.8
./configure --with-mysql=/usr/local/mysql
make
make install
cp etc/barnyard2.conf /etc/snort
vi /etc/snort/barnyard2.conf
Ahora se localiza la frase config hostname y se modifica
Se cambia "thor" por "localhost"

Se busca "config interface" en el mismo archivo, en esta línea debe aparecer eth0
En la línea en que aparece la frase output database se debe editar y asignar los siguientes parámetros:
alert, mysql, user=snort password=5n0rt& dbname=snort host=localhost
Se levantan nuevamente mysql y snort
Se ingresa el siguiente comando en una terminal:

snort -c /etc/snort/snort.conf -i eth0

Se abre una nueva terminal y se inserta el siguiente comando
ls -la /var/log/snort
el resultado es:

```
total 12
drwxr-xr-x  2 snort snort 4096 may 12 18:59 .
drwxr-xr-x 22 root  root  4096 may 12 18:27 ..
-rw-------  1 snort snort    0 abr 20 19:20 alert
-rw-r--r--  1 root  root    39 abr 20 20:11 barnyard.waldo
-rw-------  1 root  root     0 may 12 18:59 snort.log.1273708766
```

Ahora se tiene que copiar el último numero de snort.log
En este caso 1273708766
cd /var/log/snort
Si no existe el archivo barnyard.waldo, lo creamos
vi barnyard.waldo
Se insertan las siguientes líneas y se guardan los cambios:

/var/log/snort
snort.log
<el numero de 10 digitos arriba mencionado (1273708766
)>
0

Si tratamos de iniciar barnyard nos mandara el siguiente error
ERROR: Stat check on log dir (/var/log/barnyard2) failed: No such file or directory.
Fatal Error, Quitting..
Para evitar dicho error creamos el directorio donde se guardara la bitacora de barnyard
mkdir /var/log/barnyard2
iniciamos barnyard:

/usr/local/bin/barnyard2 -c /etc/snort/barnyard2.conf -G /etc/snort/gen-msg.map -S /etc/snort/sid-msg.map -d /var/log/snort/ -f snort.log -w /var/log/snort/barnyard.waldo

Ahora probamos Snort
Se tiene que crear una regla para probar Snort en el archivo local.rules
Las reglas locales son reglas que el administrador de snort escribe él mismo y se tiene la convención de iniciar con SID (Snort ID) de 1,000,000-1,999,999.

Se tiene que abrir una tercera terminal y editar el archivo local.rules
vi /etc/snort/rules/local.rules

Se agrega la siguiente línea:
alert tcp any any <> any 80 (msg: "Test web activity"; sid:1000001;)

Se guardan los cambios y se debe reiniciar Snort.
Ahora abrimos un navegador de Internet, visitamos cualquier sitio y en la interfaz oprimimos Ctrl + c para detener snort y ver lo que ha monitoreado.

Ahora se tiene que abrir BASE
El directorio a abrir por default debe ser /var/www/html, para ello se debe modificar la siguiente línea en el archivo httpd.conf:

DocumentRoot "/var/www/html"
Después se ingresa la siguiente dirección en un navegador web: http://localhost/base-1.4.5 y vemos los eventos detectados, si vemos eventos con un número SID 1000001 snort funciona correctamente, figura 4.14, Alertas en BASE.
Ahora se tiene que deshabilitar la regla que acabamos de crear.

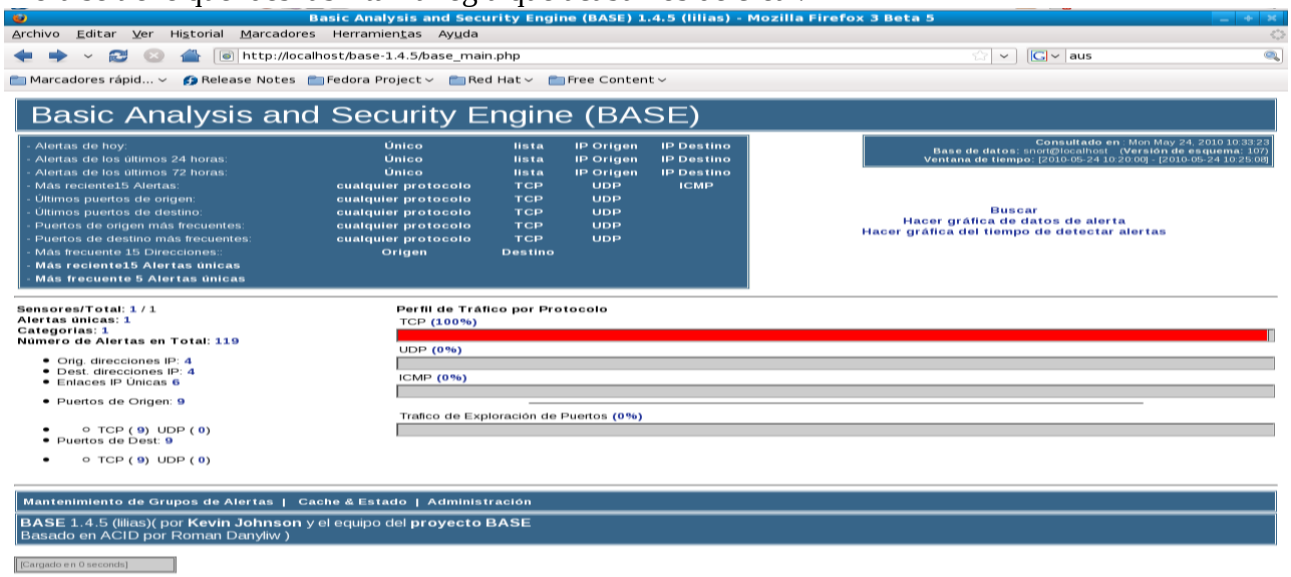


Figura 4.14, Alertas en BASE.

Hasta este momento se ha logrado hacer la instalación y configuración de las herramientas del sistema de defensa que se emplearán para monitorear todos los eventos en la red, en el siguiente capítulo, denominado, pruebas del sistema de defensa, se realizan una serie de pruebas sobre diferentes elementos de dicho sistema para verificar que la instalación y configuración de las herramientas sean las óptimas para obtener el máximo rendimientos de las mismas.