ASEGURANDO ISSABEL PBX "LA RECETA"

La Receta para el aseguramiento de Issabel PBX

JUAN OLIVA

SECURITY CONSULTANT

[PRIMERA EDICIÓN]
Junio de 2017

Modificaciones y sugerencias de la obra a joliva@silcom.com.pe

Primera Edición

Dedicado a mis padres Juan y María

1. Agradecimiento

El desarrollo de este documento no hubiera sido posible, sin el apoyo y confianza de:

Proyecto de Issabel www.issabel.org por invitarme a brindar la charla en el #BeFree17 www.befreeit.world cuya presentación que realicé inspiro este contenido.

A mi esposa y mi hijo, que gracias a su paciencia y cariño, me proporcionan la inspiración para seguir adelante.

2. Acerca del autor

Juan Oliva Córdova
Jefe de Proyectos e Ingeniería
Silcom VoIP Security Assessment

Acerca de SILCOM, empresa peruana dedicada a seguridad informática y Telefonía IP. La cual cuenta con más de 15 años de experiencia en el mercado, desarrollando proyectos para empresas nacionales y del extranjero.

Juan, es especialista en seguridad informática a nivel senior, ha realizado pruebas de penetración y Ethical Hacking para entidades del gobierno y del sector financiero, así como en entidades nacionales y del extranjero.

Se encuentra especializado en hacking de servicios de Voz sobre IP (VoIP) donde ha conseguido mostrar las graves vulnerabilidades que existen respecto a estos elementos. Ponente de eventos nacionales e internacionales desde hace varios años mantiene un blog personal http://jroliva.wordpress.com el cual se ha convertido un punto de consulta obligatorio, sobre temas seguridad informática, cuenta con certificaciones vigentes en Hacking y Linux.

3. Introducción

El objetivo del presente documento es guiar de una manera muy sencilla, en la mejora de algunos aspectos relacionados con la seguridad de la plataforma de comunicaciones Issabel PBX, tanto para servidores implementados en la nube, así como en instalaciones locales.

Acerca de Issabel PBX
Es una plataforma de comunicaciones Software Libre y código abierto basada en Asterisk (Digium the Asterisk Company) integra funcionalidades de PBX, correo electrónico, tareas de colaboración, así como video llamadas.

Todas las instrucciones del presente material fueron realizadas con la versión que corresponde al archivo ISO issabel4-USB-DVD-x86_64-20170621.iso.

Juan Oliva
SILCOM

Índice de Contenidos

[PAGINA DEJADA INTENCIONALMENTE EN BLANCO]

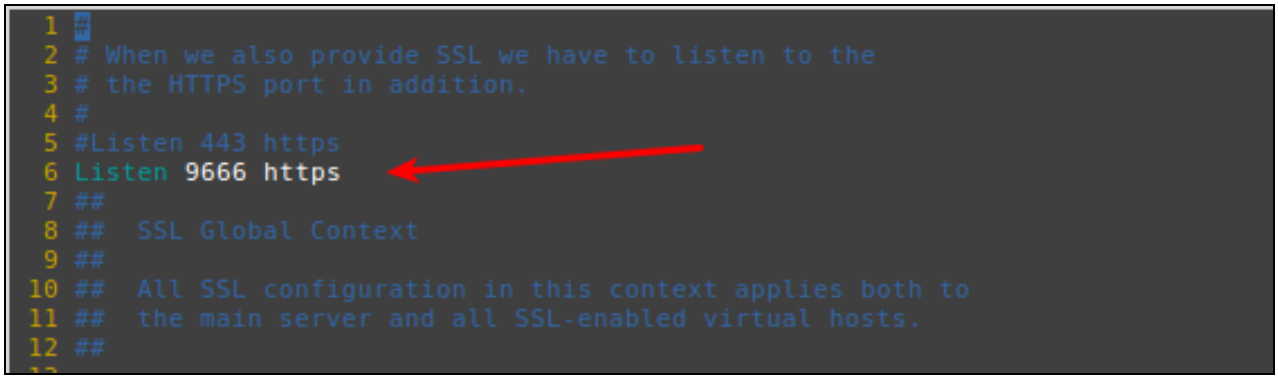
ASEGURAMIENTO DE ISSABEL PBX – LA RECETA

4. Ingrediente1 - Cambiar el puerto por defecto del servidor web

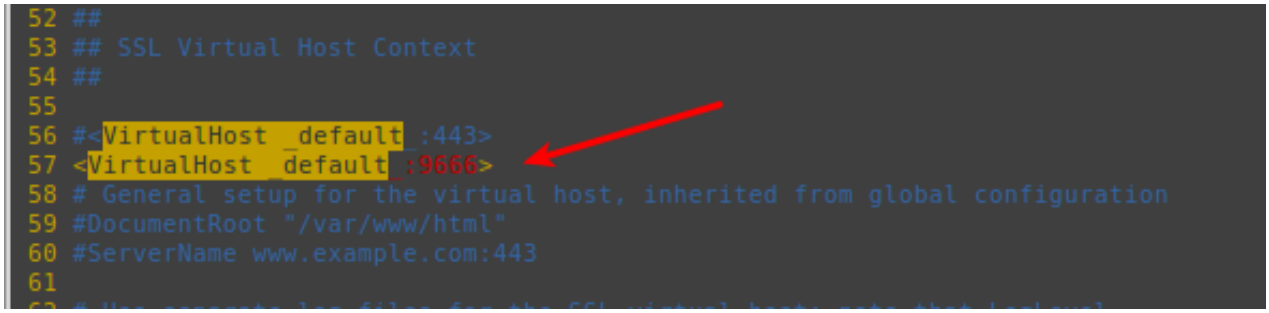
El objetivo de este ingrediente es evitar que programas que realizan escaneos de puertos, detecten fácilmente la interface web de la plataforma y puedan desarrollar ataques a la misma.

vi /etc/httpd/conf.d/ssl.conf

Cambiar el parámetro "Listen 443 https" donde 443 es el puerto de escucha por defecto, en el ejemplo se usa el puerto 9666.



Luego cambiar el parámetro "virtualHost_default :443" por "virtualHost_default :9666" es necesario que el puerto sea el mismo que el usando en el parámetro "Listen"

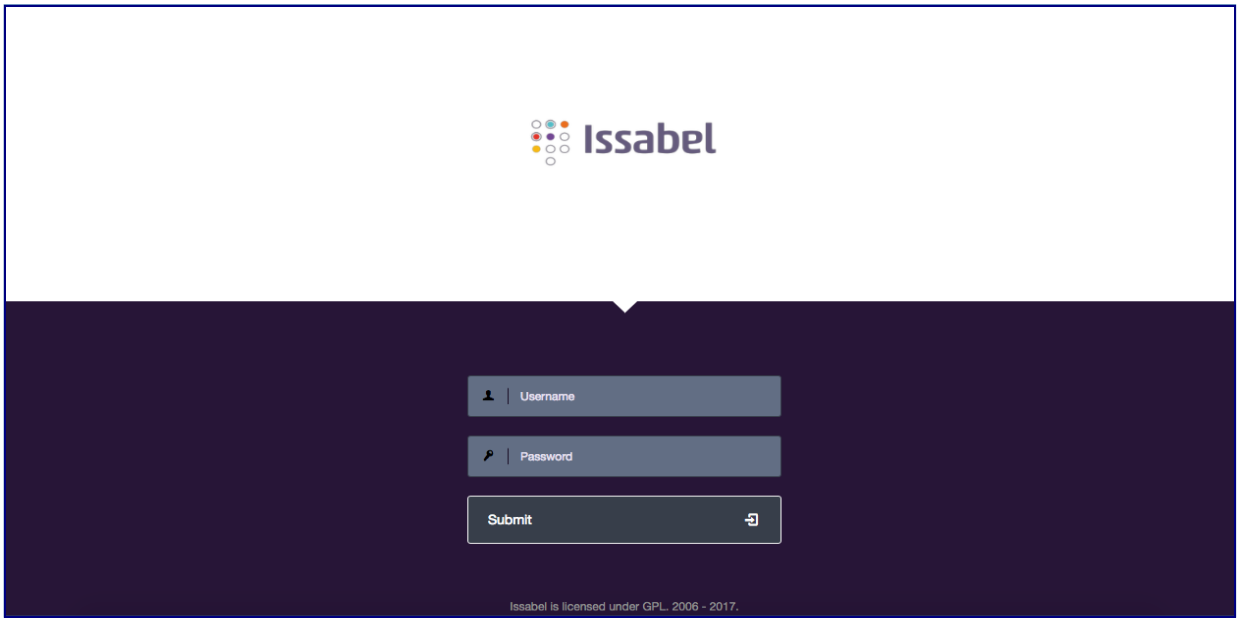


Finalmente reiniciar el servicio de web

service httpd restart

Probar el resultado:

Ingresar a la interface web de la siguiente forma: https://192.168.1.10:9696



5. Ingrediente 2 - Configurar doble autenticación web

El propósito de configurar un nivel adicional de autenticación en el servicio web, es proteger de manera integral todas las aplicaciones y carpetas que estén publicadas en este servicio, de esta forma impedir el ingreso de exploits remotos que atacan por este vector.

vi /etc/httpd/conf.d/issabel.conf

Agregar los parámetros para que el servicio web solicite autenticación, de la siguiente forma:

```
AuthType Basic
AuthName "Zona Restringida"
AuthUserFile /usr/www/wwwpasswd
Require user issabel
```

```
# Apache-level configuration for Elastix administration interface

Timeout 300

# Default apache configuration specifies greater limits than these
#MaxClients       150
#MaxRequestsPerChild  1000

# Default apache User and Group diretives MUST be commented out
# in order for these to take effect.
User asterisk
Group asterisk

<Directory "/var/www/html">
    # Redirect administration interface to https
    RewriteEngine On
    RewriteCond %{HTTPS} off
    RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
    AuthType Basic
    AuthName "Zona Restringida"
    AuthUserFile /var/www/wwwpasswd
    Require user issabel
</Directory>
```

Luego crear el usuario declarado para este ejemplo: “issabel”

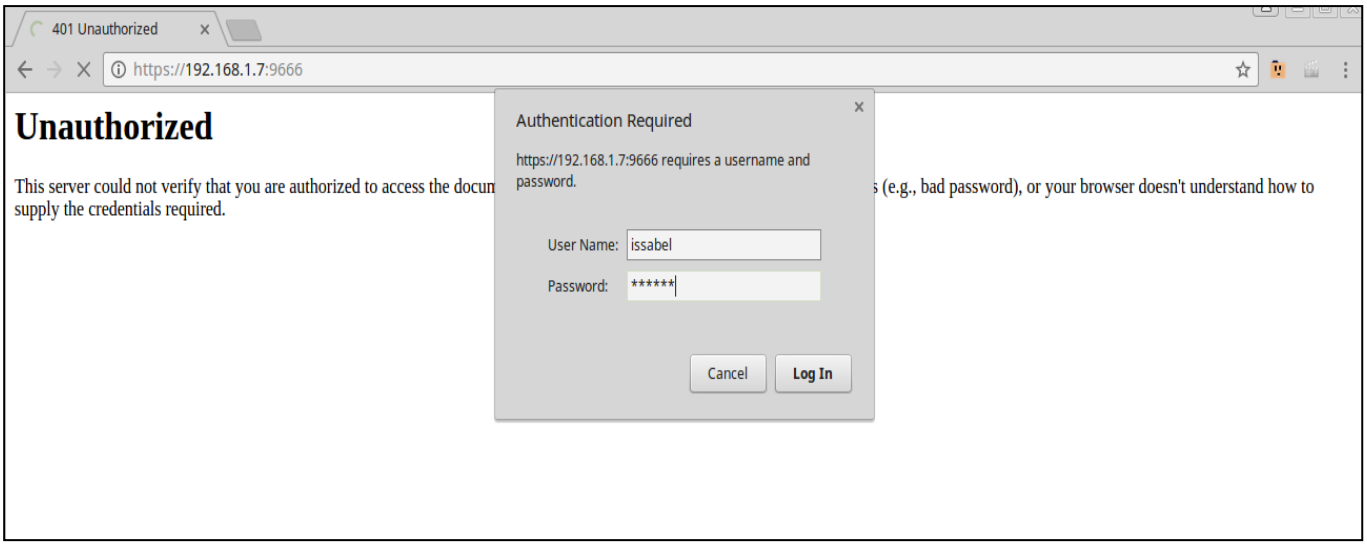
htpasswd -c /usr/www/wwwpasswd issabel
password: clavedeusuario

```
[root@isapbx4b2 www]#
[root@isapbx4b2 www]#
[root@isapbx4b2 www]# htpasswd -c /var/www/wwwpasswd issabel
New password:
Re-type new password:
Adding password for user issabel
[root@isapbx4b2 www]#
[root@isapbx4b2 www]#
```

service httpd restart

Probar el resultado:

Ingresar a la interface web solicitará autenticación de la siguiente forma



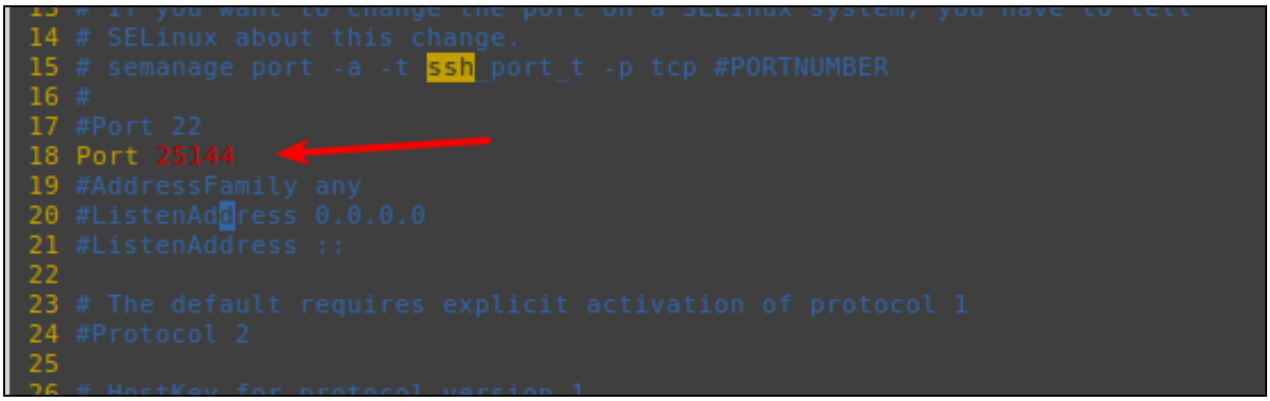
6. Ingrediente 3 - Configuración de servicio SSH

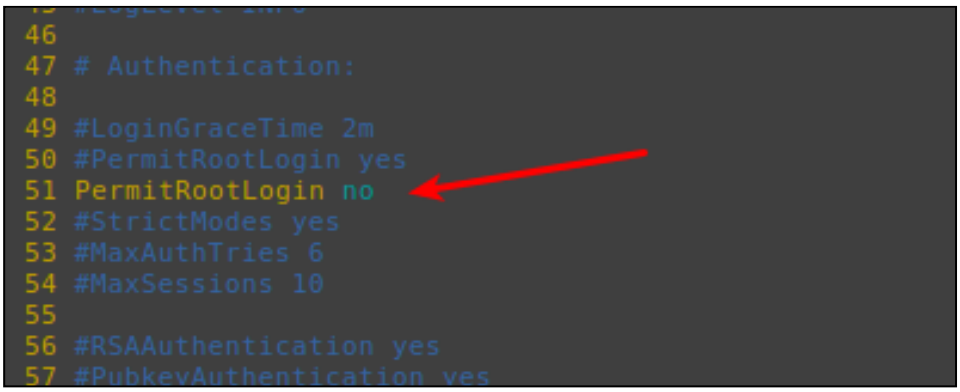
Configurar adecuadamente el servicio SSH es una tarea primordial, debido a que representa un punto de acceso a toda la plataforma, para ello es necesario cambiar el puerto por defecto y evitar el acceso al usuario "root" de la siguiente forma:

```
vi /etc/ssh/sshd_config
```

Cambiar el puerto por defecto del servicio SSH, de la siguiente forma:

```
Port 25144
PermitRootLogin no
```



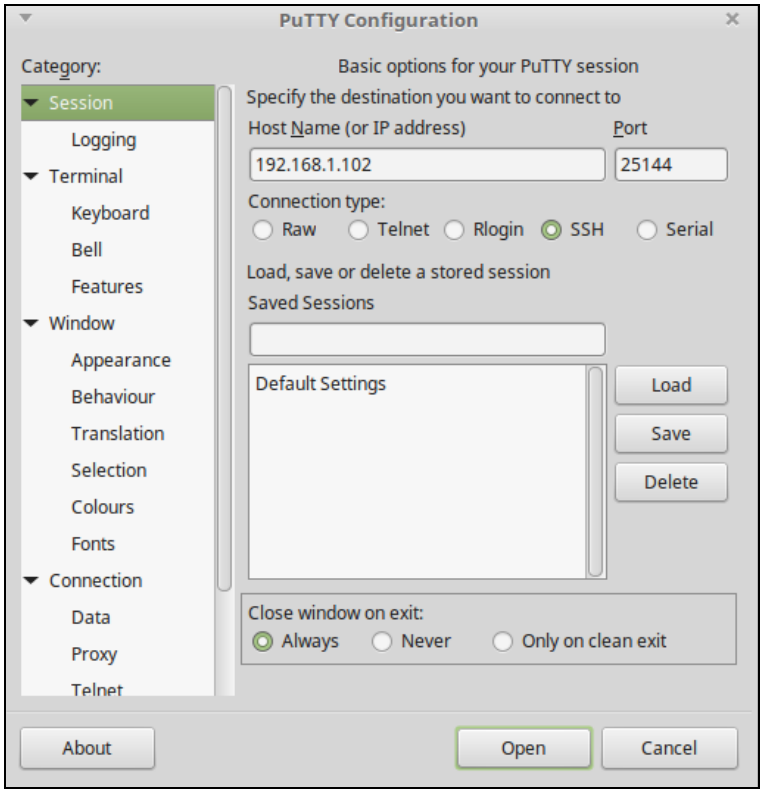


Luego cambiar el agregar un usuario del sistema, establecer la contraseña y finalmente reiniciar el servicio SSH

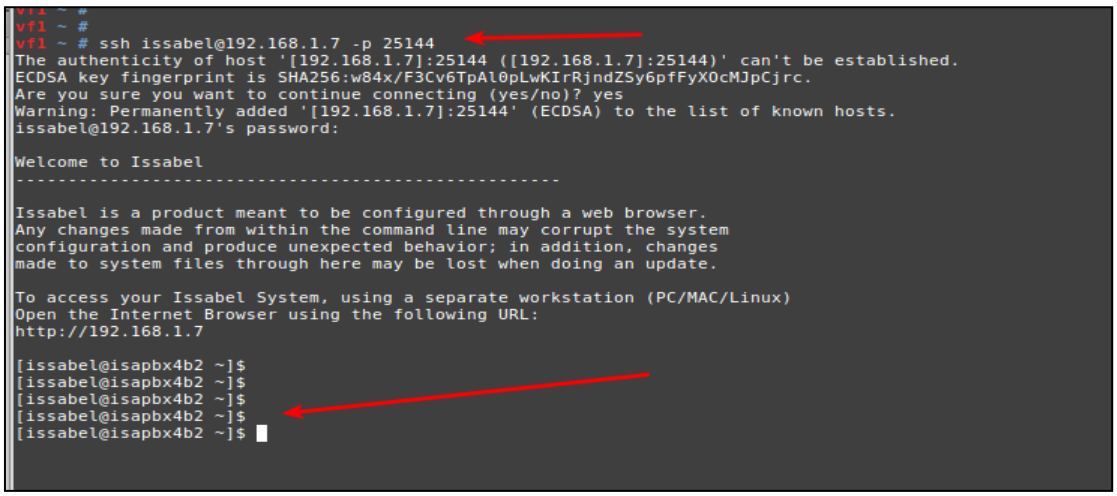
```
adduser issabel
passwd issabel
service sshd restart
```

Probar el resultado:

Ingresar al servicio se deberá indicar el nuevo puerto configurado para el servicio SSH, de la siguiente forma:



Luego ingresar con el usuario creado, ya que no será posible ingresar con el usuario root por defecto.

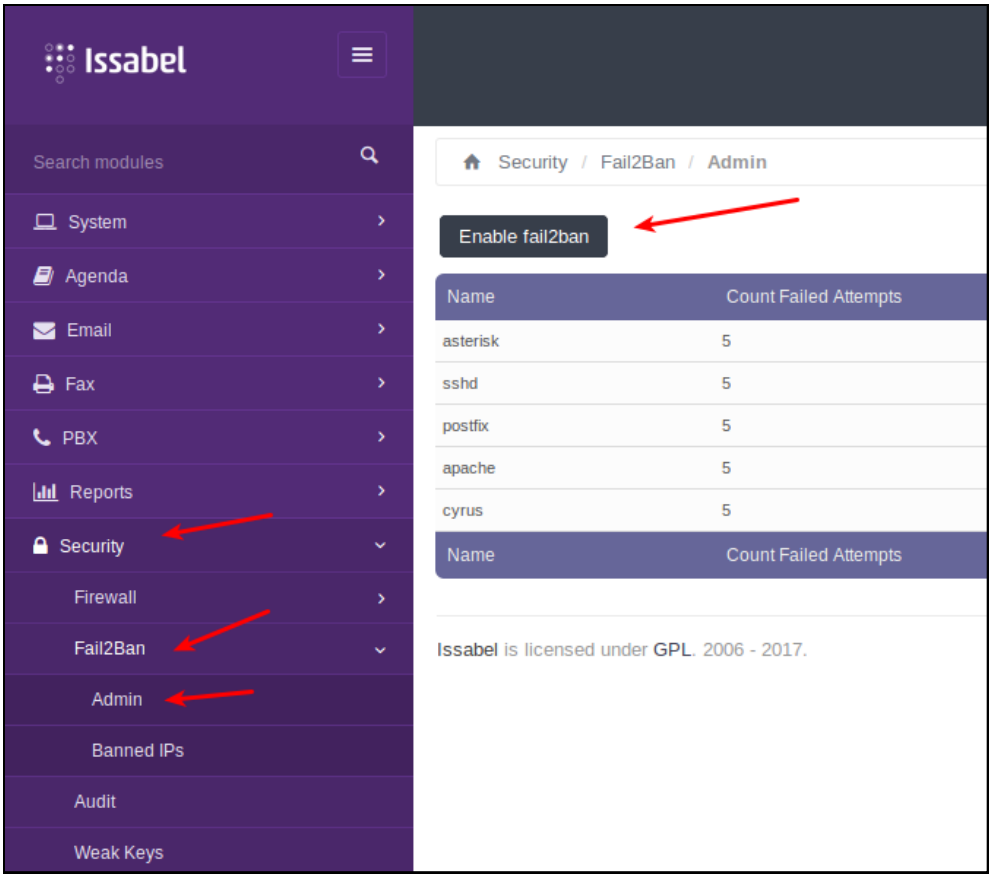


7. Ingrediente 4 - Configuración de Fail2ban

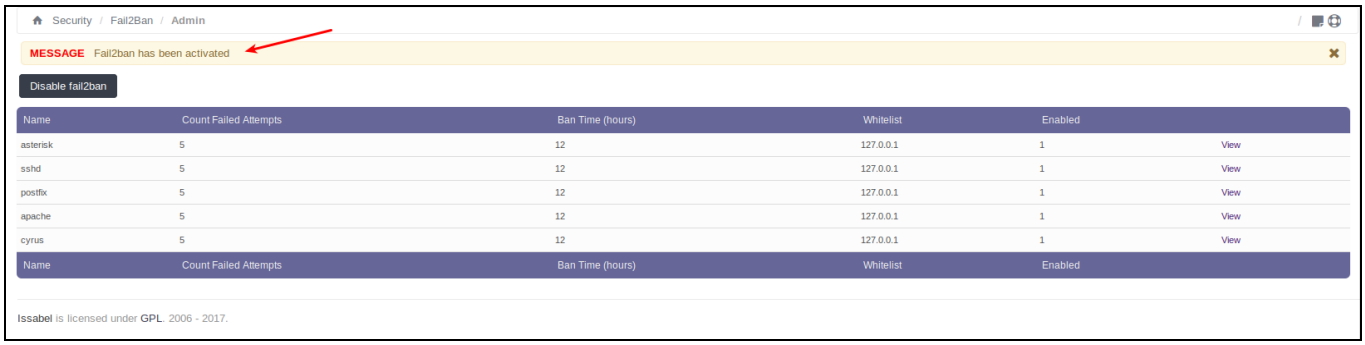
Fail2ban es un elemento imprescindible para la protección, no solo de una plataforma de comunicación basada en Asterisk, sino de toda plataforma basada en Linux, ya que provee protección proactiva (bloqueo automático) ante ataques externos y/o internos.

En el caso de Issabel, Fail2ban ya viene instalado y configurado para proteger servicios como el protocolo SIP de Asterisk y SSH respectivamente.

Para activar el servicio es necesario ingresar a Security / Fail2ban / Admin y luego hacer clic sobre el botón “Enable Fail2ban” de la siguiente forma:



Luego tendremos el servicio activado de la siguiente forma



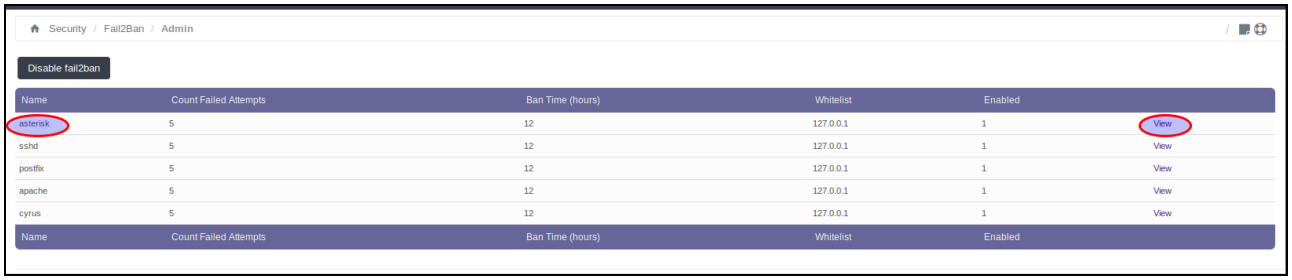
También podremos ver que FAIL2BAN colabora perfectamente con IPTABLES con el siguiente comando:

```
[root@pbx ~]#
[root@pbx ~]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
f2b-asterisk-ami  tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 5038
f2b-asterisk-udp  udp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 0:65535
f2b-asterisk-tcp  tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 0:65535
f2b-postfix-sasl  tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 25,465,587,220,993,110,995
f2b-postfix  tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 25,465,587
f2b-apache-shellshock  tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 80,443
f2b-apache-modsecurity  tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 80,443
f2b-apache-fakegooglebot  tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 80,443
f2b-apache-botsearch  tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 80,443
f2b-apache-nohome  tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 80,443
f2b-apache-overflows  tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 80,443
f2b-apache-noscript  tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 80,443
f2b-apache-badbots  tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 80,443
f2b-apache-auth  tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 80,443
f2b-sshd-ddos  tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 22
f2b-sshd   tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 22

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain f2b-apache-auth (1 references)
target     prot opt source               destination
RETURN     all  --  0.0.0.0/0            0.0.0.0/0

Chain f2b-apache-badbots (1 references)
target     prot opt source               destination
RETURN     all  --  0.0.0.0/0            0.0.0.0/0

Chain f2b-apache-botsearch (1 references)
target     prot opt source               destination
RETURN     all  --  0.0.0.0/0            0.0.0.0/0

Chain f2b-apache-fakegooglebot (1 references)
target     prot opt source               destination
RETURN     all  --  0.0.0.0/0            0.0.0.0/0

Chain f2b-apache-modsecurity (1 references)
target     prot opt source               destination
RETURN     all  --  0.0.0.0/0            0.0.0.0/0

Chain f2b-apache-nohome (1 references)
target     prot opt source               destination
RETURN     all  --  0.0.0.0/0            0.0.0.0/0

Chain f2b-apache-noscript (1 references)
target     prot opt source               destination
RETURN     all  --  0.0.0.0/0            0.0.0.0/0

Chain f2b-apache-overflows (1 references)
target     prot opt source               destination
RETURN     all  --  0.0.0.0/0            0.0.0.0/0

Chain f2b-apache-shellshock (1 references)
target     prot opt source               destination
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
```

Como podemos ver ahora FAIL2BAN está colaborando perfectamente con IPTABLES, se puede apreciar que ahora el servicio está protegiendo no solo Asterisk y SSH si no también otros servicios como el servidor web Apache.

Es posible gestionar la protección de cada servicio editando de la siguiente forma

Editar el servicio Asterisk haciendo clic sobre el botón “View”



Dentro del servicio hacer clic sobre el botón “Edit”

Ahora es posible configurar parámetros como:

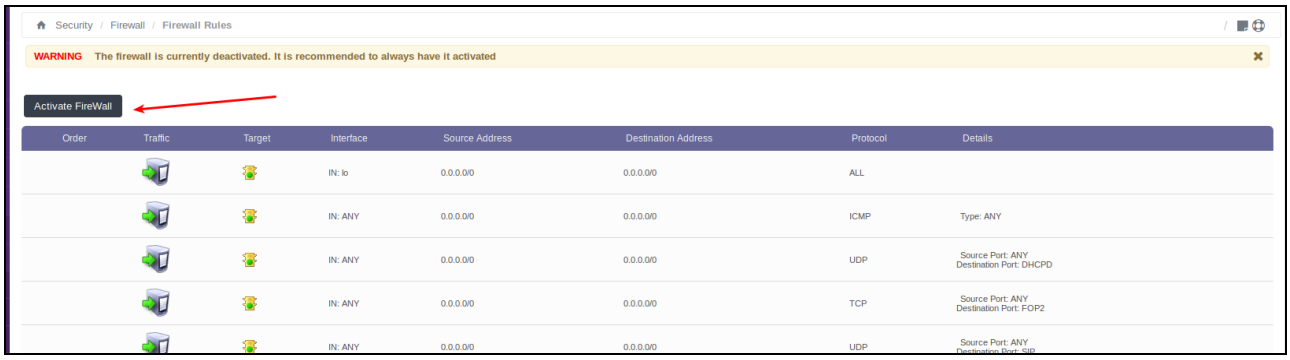
Count failed Attempts: Cantidad de intentos fallidos antes generar el bloqueo de la IP
Ban Time : Cantidad de horas en la que la dirección IP estará bloqueada
Whitelist : Direcciones IP o segmentos que no serán tomados en cuenta para bloquear.
Enabled: Activar o desactivar la protección del servicio en Fail2ban.

Finalmente hacer clic en el botón “Save” para guardar los cambios.

8. Ingrediente 5 - Configuración de Firewall

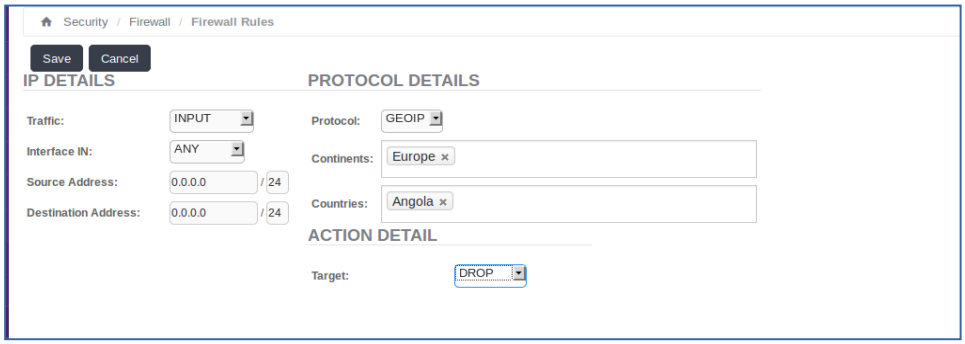
El Firewall sigue siendo un elemento importante en la configuración de seguridad.

Para activar el servicio es necesario ingresar a Security / Firewall / Firewall Rules y luego hacer clic sobre el botón “Activate Firewall” de la siguiente forma:



Las reglas que activa el Firewall están preparadas para no comprometer el acceso a los recursos que ofrece la plataforma, así mismo es posible que trabaje totalmente compatible con Fail2ban.

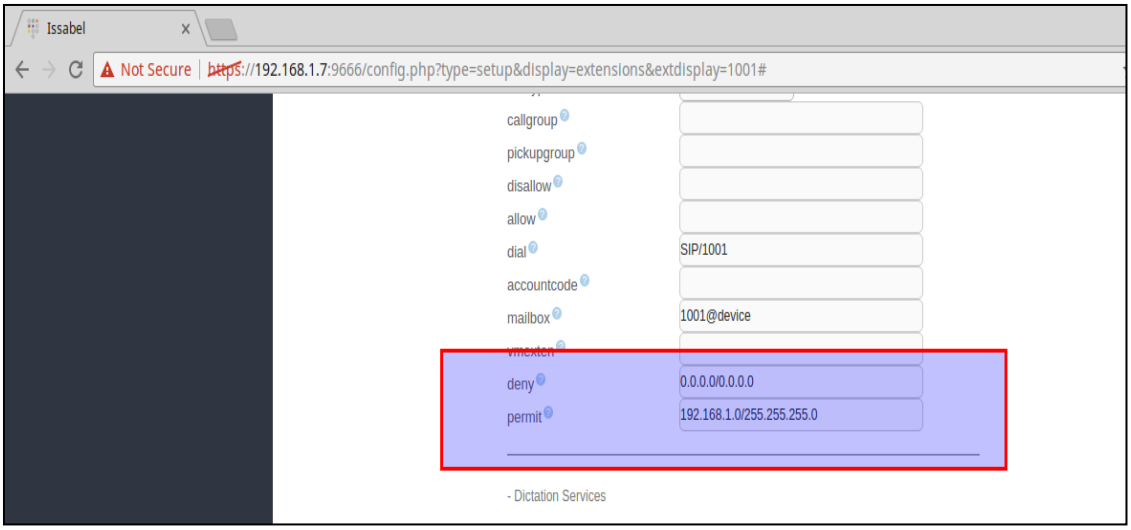
Es posible crear una regla para bloquear tráfico por geo localización, por ejemplo para el caso que deseemos bloquear tráfico entrante o saliente de un país o países en específico, como se muestra a continuación:



9. Ingrediente 6 - Configuración de ACL a nivel SIP

Una práctica muy buena es crear reglas de control de acceso a nivel de las extensiones SIP de tal forma que solo podrán “registrarse” a estas las direcciones IP o rangos de IP

Para activar es necesario editar cada una de las extensiones, como por ejemplo la 1001 de la siguiente forma:



Tener en cuenta que para instalaciones en la nube, este tipo de ajuste puede causar inconveniente, ya que los anexos o extensiones pueden registrarse desde redes donde las direcciones IP públicas pueden dinámicas.

Nota del autor: Esta configuración no es apta para administradores soporíferos.

10. Ingrediente 7 - Alertas para llamadas internacionales

Lo interesante de una plataforma de comunicaciones basada en Asterisk es que puedes modificarla a tu gusto y necesidad.

El siguiente código proporciona la capacidad de enviar un email cuando se realiza una llamada internacional.

```
1) exten=>_0.,n,System(/bin/echo "Llamada LDN al numero ${NUMERO}  Del usuario : ${CONTRASENA} Realizada : ${calltime} " >
/etc/asterisk/email.txt)
2) exten=>_0.,n,System(/bin/mail -s ALERTA-LLAMADA-LDN joliva@silcom.com.pe</etc/asterisk/email.txt)
3) exten=>_0.,n,Dial(SIP/TRONCAL/${NUMERO})
```

Primera línea, crea el archivo email.txt con las variables de canal en él.
Segunda línea, envía el correo adjuntando el archivo email.txt
Tercera línea, realiza la llamada.

11. Ingrediente 8 - Alertas ante cambio de configuraciones

Monitorear los eventos que suceden en el sistema de archivos y más aún los archivos relacionados con la plataforma, es una tarea sumamente importante. INCROND es un servicio que notifica sobre los cambios que pueden suceder en dentro de una carpeta o un archivo en específico.

Usando este programa, vamos a monitorear si existen cambios en los archivos extensions_curstom.conf o sip_general.conf, o siquiera fueran fueran abiertos de alguna forma y además que les enviara alertas al correo en caso de recibir esos eventos.

Primero instalar el servicio

```
yum -y install incron
service incrond start
vim /etc/incron.d/monitor_archivos_issabel
```

Luego de crear/editar el archivo "monitor_archivos_issabel" y agregar el siguiente contenido

```
/etc/asterisk IN_MODIFY /root/incrond/incrond_email.sh $@ $# $%
```

Lo que hace el archivo lo siguiente:
/etc/asterisk : Carpeta a monitorear
IN_MODIFY : Evento que deseamos monitorear en este caso modificación.
/root/incrond/incrond_email.sh : Script al cual vamos a enviar los parámetros que se disparan al activarse el evento
$@ : path del fichero o directorio.
$# : Nombre del fichero o directorio, sin el path.
$% : Nombre del evento que se disparó

Ahora vamos a crear el archivo "incrond_email.sh" el cual va recibir los parámetros definidos en el archivo de configuración "monitor_archivos_issabel"

```
mkdir /root/incrond
touch /root/incrond/incrond_email.sh
vim /root/incrond/incrond_email.sh
```

```
#!/bin/bash
/bin/echo "ALERTA DE MONITOR DE ARCHIVOS / Se ha producido cambios en los archivos del servidor ISSABEL , los detalles son : Ruta archivo modificado: $1 Nombre archivo modificado: $2 Evento/Accion: $3 \n" > /root/incrond/incrond_email.txt
/bin/mail -s ALERTA-MODIFICACION-ARCHIVOS jroliva@gmail.com</root/incrond/incrond_email.txt
```

Luego agregar una función horaria para que el servicio solo se ejecute fuera de horarios laborales (opcional)

```
vi /root/incrond/incrond_funcionhoraria.sh
```

```
#!/bin/bash
HORA=$(date +%H)
echo $HORA

if [ $HORA > 18 ]; then
/sbin/service incrond start
else
/sbin/service incrond stop
Fi
```

Automatizando vía crontab

```
chmod a+x  /root/incrond/incrond_funcionhoraria.sh
crontab -e
*/60 *    * * *    /root/incrond/incrond_funcionhoraria.sh
```

FINALMENTE

"Júntense todos los ingredientes y tendrá como resultado una plataforma bastante segura"

12. Referencias y Bibliografía

Proyecto Issabel
http://www.issabel.org

Asterisk
http://www.asterisk.org

Juan Oliva Blog
http://jroliva.net

Incron
http://inotify.aiken.cz/?section=incron&page=about&lang=en