

Arquitectura de Sistemas Computarizados
Instalación de Firewall bajo Linux
Trabajo práctico

1. [Introducción](#)
2. [IP Tables](#)
3. [Distribución](#)
4. [Test de penetración](#)
5. [Solución de intrusión](#)
6. [Conclusiones](#)
7. [Bibliografía](#)

Introducción

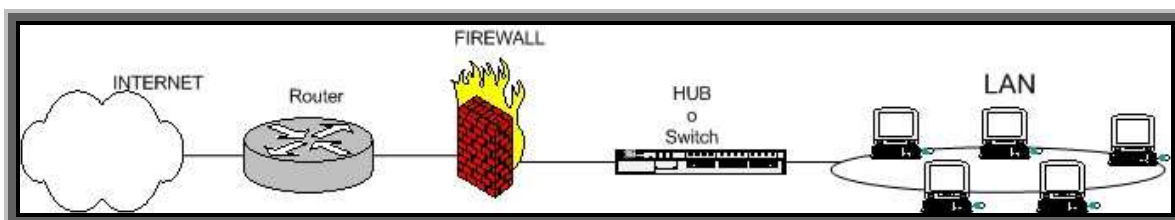
El siguiente documento tiene como objetivo describir y documentar el trabajo practico realizado por los alumnos, Darreche Esteban, Ordoñez Javier, Camisar Fernando Andres Alfredo Berner y Jaca Pablo.

La cátedra ha solicitado que a fin de que logremos adquirir experiencia en el manejo de Linux propongamos un tema a tratar que tenga que ver con el uso de dicho sistema operativo y realizemos una demostración de la aplicación practica que se puede dar al tema elegido.

El tema que ha elegido el grupo es la aplicación de tecnología basada en Linux para brindar servicios de configuración dinámica, acceso a Internet, y Proxy a una red de área local (LAN) garantizando un buen nivel de seguridad.

1.1. Objetivo

El objetivo del trabajo es demostrar como se puede implementar a bajo costo y reciclando hardware un sistema que permita el acceso seguro a Internet y la conectividad entre computadoras mediante sistemas linux.



La idea es configurar un equipo bajo el sistema operativo Linux para que cumpla la función de Router y el Firewall.

1.2. Roles en la presentación.

Introducción

Durante este periodo de la presentación se explicara cuales son los temas que vamos a tratar, el objetivo del trabajo y se presentara a los integrantes del grupo.

Encargado Fernando Camisar

IP-Tables

Durante este periodo de la presentación se explicara que es IP-TABLES y como funciona, por que hemos elegido esta tecnología y se realizara una comparación con tecnologías anteriores.

Encargado Esteban Darreche

Distribución.

Durante este periodo de la presentación se mostrara la distribución que hemos elegido, se explicara como se instalo, como se configura, que formas de administración tiene, que servicios provee, que tecnologías utiliza y como trabaja.

Encargado Javier Ordoñez

Test de penetración.

Este periodo de la presentación se dividirá en dos partes con el fin de mostrar en tiempo real el funcionamiento del firewall, se va a atacar a una PC primero sin el firewall mediante software especializado en seguridad, y luego con el firewall activado, luego se compararan los resultados en las dos etapas para que se pueda notar como el firewall permite proteger la red.

También se explicara el funcionamiento del software utilizado en el ataque.

Encargados:

Ataque sin firewall Andres Berner

Ataque con firewall Pablo Jaca

Solución de intrusión.

Este periodo de la presentación será la contraparte de el periodo anteriormente explicado, se mostrara como a medida que se reciben los ataques el firewall los detecta y se explicara que tipo de ataque se ha detectado.

Por otro lado se explicara el funcionamiento de el IDS utilizado por el firewall en ente caso SNORT.

Encargados:

Análisis de detección de intrusión..... Fernando Camisar

Explicación de IDS y SNORT Mariano Crimmi

Conclusiones

Se expondrán las conclusiones obtenidas tras la el trabajo y se responderán preguntas.

Encargado Pablo Jaca

2. IP Tables

La tecnología seleccionada para cumplir nuestro objetivo ha sido IP Tables.

A continuación daremos una breve explicación de su forma de trabajo.

El software de filtrado de paquetes denominado IP-Tables existe en las versiones de kernel 2.4 en adelante, estos son algunos otros métodos que se utilizaban anteriormente y las versiones de kernel que los contienen.

En los Kernel de versiones 2.1.X el paquete de filtrado es el IP-FWADM.

En los Kernel de versiones 2.2.X el paquete de filtrado es el IP-CHAINS.

En los Kernel de versiones 2.4.X el paquete de filtrado es el IP-TABLES.

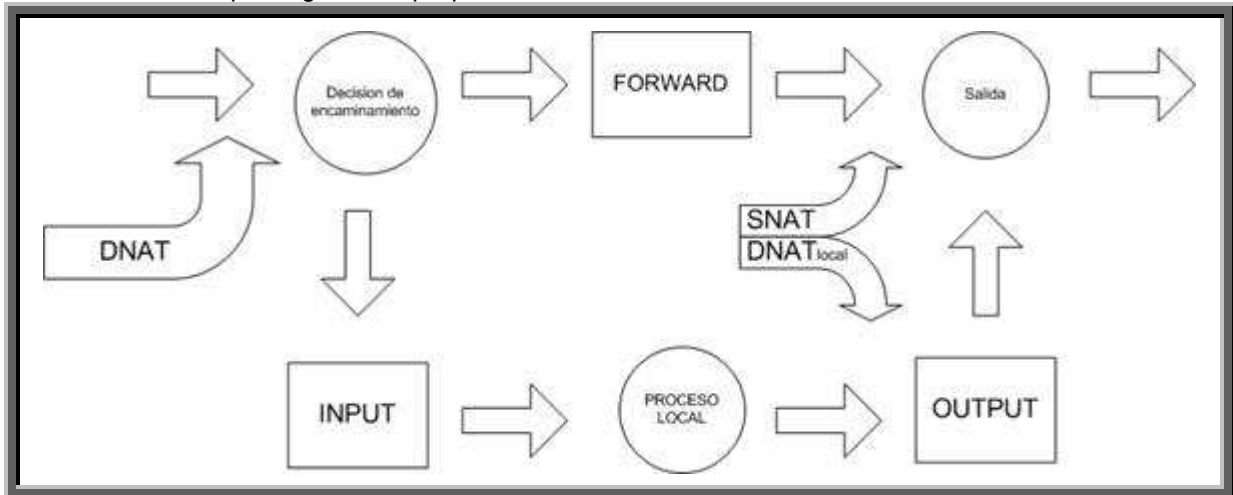
IPtables es un sistema de firewall vinculado al kernel de linux que se ha extendido enormemente a partir del kernel 2.4 de este sistema operativo. Al igual que el anterior sistema ipchains, un firewall de iptables no es como un servicio que iniciamos o detenemos o que se pueda caer por un error de programación (esto es una pequeña mentira, ha tenido alguna vulnerabilidad que permite DoS, pero nunca tendrá tanto peligro como las aplicaciones que escuchan en determinado puerto TCP): iptables está integrado con el kernel, es parte del sistema operativo. Para utilizar IP Tables lo que se hace es aplicar reglas mediante la ejecución del comando iptables, con el que añadimos, borramos, o creamos reglas. Por ello un firewall de iptables no es sino un simple script de shell en el que se van ejecutando las reglas de firewall.

Se puede implementar un script de inicio en /etc/rc.d/INIT.d (o /etc/INIT.d) con el que se puede lograr que iptables se "inicie o pare" como un servicio más. Lo podemos hacer nosotros o es probable que venga en la distribución (como en redhat por ejemplo). También se pueden salvar las reglas aplicadas con el comando iptables-save en un archivo y gestionar ese archivo con una aplicación o front-end desde la X o desde la web.

Ejemplo de funcionamiento:

Tenemos una máquina linux con soporte para iptables, tiene reglas aplicadas y empiezan a llegar/salir/pasar paquetes. No le daremos importancia a la cantidad de placas de red, direcciones ip y si los paquetes son entrantes o salientes. Las reglas de firewall están a nivel de kernel, y al kernel lo que le llega es un paquete y tiene que decidir que hacer con él. El kernel lo que hace es, dependiendo si el paquete es para la propia máquina o para otra máquina, consultar las reglas de firewall y decidir que hacer con el paquete según lo que establezcan dichas reglas.

Este es el camino que seguiría un paquete en el kernel:



Cuando un paquete u otra comunicación llega al kernel con iptables se sigue este camino

Como se ve en el gráfico, básicamente se mira si el paquete está destinado a la propia máquina o si va a otra. Para los paquetes (o datagramas, según el protocolo) que van a la propia máquina se aplican las reglas INPUT y OUTPUT, y para filtrar paquetes que van a otras redes o máquinas se aplican simplemente reglas FORWARD.

INPUT, OUTPUT y FORWARD son los tres tipos de reglas de filtrado. Pero antes de aplicar esas reglas es posible aplicar reglas de NAT: estas se usan para hacer redirecciones de puertos o cambios en las IPs de origen y destino.

E incluso antes de las reglas de NAT se pueden aplicar reglas de tipo MANGLE, destinadas a modificar los paquetes; aunque son reglas poco conocidas y no utilizadas frecuentemente nos pareció que vale la pena mencionarlas.

Por lo tanto tenemos tres tipos de reglas en iptables:

- MANGLE
- NAT: reglas PREROUTING, POSTROUTING
- FILTER: reglas INPUT, OUTPUT, FORWARD.

Ventajas de configurar linux como Firewall

- Linux es un sistema operativo gratuito.
- El equipo donde corre el firewall necesita requerimientos mínimos
- Alta fiabilidad, ya que linux presenta gran calidad y estabilidad : muchas empresas están eligiendo opciones de este tipo.
- Sobre el sistema operativo Linux se puede montar múltiples servicios tales como:
 - Servidor Proxy HTTP y FTP con cache de disco para acelerar la navegación por Internet.
 - Informes generados en forma automática.
 - Bloqueo opcional para la navegación en mas de 30.000 sitios.
 - Conversión de las direcciones IP de su red privada (NAT)

3. Distribution

La distribución elegida fue IP-COP, a continuación examinaremos esta distribución detalladamente y describiremos como fue el proceso de instalación, como se puede configurar y cuales son los métodos de administración.

3.1. Características

Estas son algunas de las principales características por las que se Eligió IP-COP:

- Segura, Estable y altamente configurable distribución basada en Firewall.
- Web Server con paginas que permiten la sencilla administración del firewall.
- Cliente DHCP que permite obtener la dirección IP automáticamente desde el ISP.

- Servidor DHCP que permite una rápida y sencilla configuración de estaciones de trabajo en la red interna.
- Proxy DNS cache, que permite incrementar la velocidad de resolución de consultas de nombre de dominio.
- Web Proxy con cache que incrementa la velocidad de navegación por web.
- Detección de intrusos para advertir ataques desde la red externa.
- Posibilidad de particionar la red en VERDE (Parte de la red protegida contra Internet) y NARANJA o DMZ (Parte de la red que contiene servidores con acceso publico parcialmente protegidos de Internet).
- VPN que permite que se conecte la red interna con otra red a través del Internet, formando una sola red lógica.

3.2. Modo de trabajo

IP-COP intenta imitar a los firewalls por hardware basándose en el concepto del firewall como una caja que cumple la única función de ser firewall pudiendo administrarse casi en su totalidad de forma remota.

Es evidente que esto no se cumple en su totalidad ya que además de la funcionalidad de firewall, a las versiones mas recientes de IP-COP se le han agregado otros servicios como DHCP y Proxy pero los creadores de la distribución siguen afirmando que cuantas mas funciones estén activas , mas vulnerable se volverá la red interna.

En IP-COP se pueden configurar 3 tipos de interfaces.

VERDE (GREEN)

Esta internase se conecta a la parte de la red que IP-COP debe proteger, se presume que detrás de esta internase habrá trafico local que para acceder a otras redes deberá pasar por el IP-COP.

NARANJA (ORANGE)

Esta partición de la red es opcional y permite que se coloquen servidores de acceso publico en una red separada. Las computadoras en esta red no pueden comunicarse con las de a red VERDE, excepto por intermedio de agujeros firmemente controlados de DMZ

El tráfico a esta red se encamina a través de una Interfase. La NIC NARANJA debe ser diferente de la NIC VERDE.

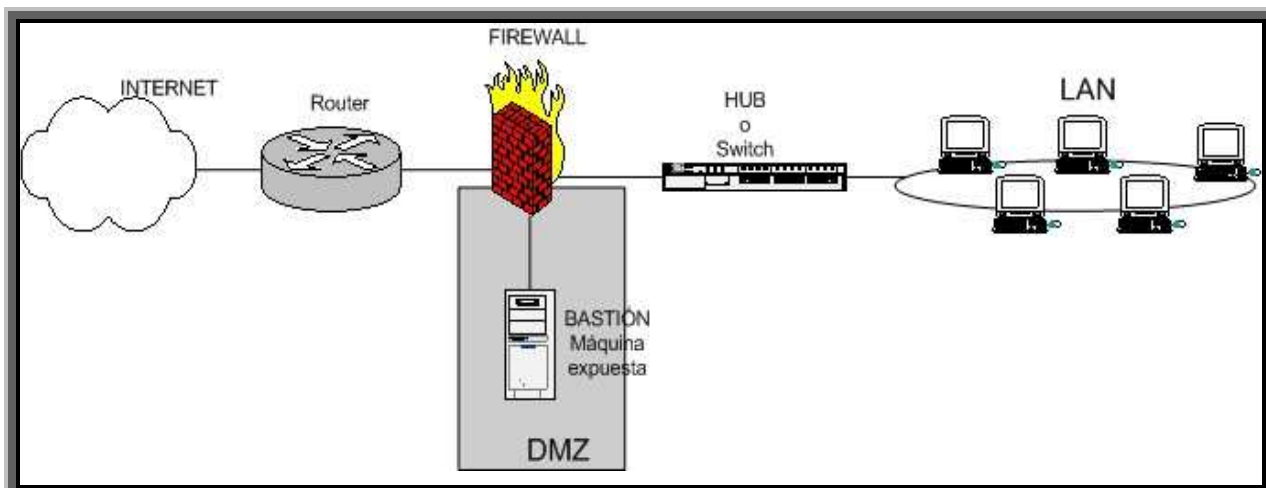
ROJA (RED)

Esta red es Internet o otra red poco confiable. El propósito primario de IP-COP es proteger la red VERDE y NARANJA y sus equipos de el trafico originado en la red ROJA.

IP-COP puede trabajar de cuatro formas diferentes.

- GREEN (RED is modem/ISDN)
- GREEN + ORANGE (RED is modem/ISDN)
- GREEN + RED (RED is Ethernet)
- GREEN + ORANGE + RED (RED is Ethernet)

Esta es la forma lógica de trabajo de IP-COP en el caso de existir una DMZ.



IP-COP realizaría los trabajos de Router y Firewall.

Firewall

IP-COP trabaja mediante IP-TABLES, esta es la tecnología mas reciente que hay en el filtrado de paquetes bajo linux implementada en las versiones de kernel superiores a la 2.4. Permite el filtrado de paquetes a través de reglas.

Proxy

Se puede configurar ipcop para que trabaje el Proxy de forma normal o transparente.

- Si el Proxy se configura en modo normal el usuario deberá configurar su browser y todos los programas que accedan a Internet con la dirección del IP-COP para la interfase VERDE. Esto permite un mayor control de las actividades del usuario.
- En cambio si el Proxy se configura en modo transparente no se requiere ningún tipo de configuración de Proxy en las estaciones de trabajo de la red interna.

3.3. Instalación

A continuación vamos a detallar las distintas formas en las que se puede llevar a cabo la instalación de la distribución IP-COP y cual fue la elegida por el grupo.

Como primer comentario debemos aclarar que IP-COP es distribuido bajo los términos de licenciamiento [GNU General Public License](http://www.gnu.org/licenses/gpl.html) especificados en <http://www.gnu.org/licenses/gpl.html>

Lo primero que se debe hacer antes de comenzar la instalación es decidir cual será la topología de la red y que funciones va a cumplir el IP-COP

Como ya hemos explicado IP-COP puede trabajar con varias configuraciones

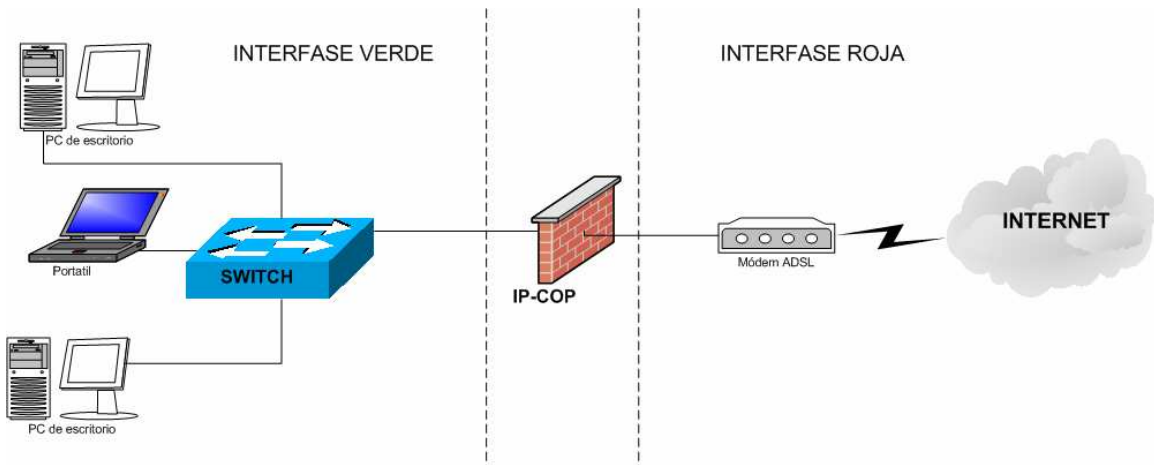
- GREEN (RED is modem/ISDN)
- GREEN + ORANGE (RED is modem/ISDN)
- GREEN + RED (RED is Ethernet)
- GREEN + ORANGE + RED (RED is Ethernet)

La configuración elegida por el grupo fue:

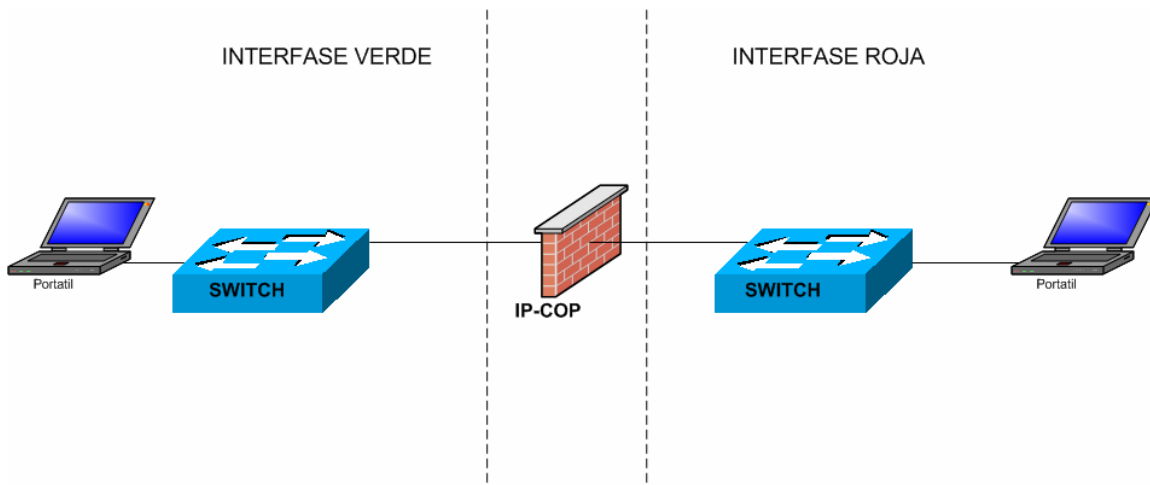
GREEN + RED (RED is Ethernet)

Esto quiere decir que vamos a tener una interfase de red Ethernet que se comunicara con la red interna (GREEN) y una interfase de red Ethernet que se comunicara por medio de un MODEM a Internet (RED).

En la practica la topología que se utiliza es la siguiente:



Tenemos 2 PC de escritorio y una portátil conectadas a un Switch ethernet que a su vez se conecta a la interfase de red (VERDE) de el firewall IP-COP. Conectado a la interfase restante (ROJA) se encuentra un MODEM ADSL que suministra la conexión a Internet. En nuestra configuración no se utiliza interfase NARANJA (DMZ) ya que no disponemos de una tercera placa de red ethernet. Debido a fines didácticos en la demostración se utilizara esta topología.



Tenemos una Portátil conectada a un switch que a su vez se conecta a la interfase VERDE de el firewall IP-COP (Esta portátil simulara a la red interna y recibirá los ataques). En la interfase ROJA del firewall conectaremos Otra portátil conectada a un switch que simulara a Internet e intentara ingresar a la red interna.

Hardware utilizado

Para la realización del proyecto se busco hardware relativamente obsoleto con el fin de demostrar la capacidad que posee linux de promocionar una gran funcionalidad reciclando equipo a bajo costo.

Especificaciones técnicas del hardware.



La configuración del hardware se basaba en una PC Compaq deskpro 5100
 Pentium 100 MHZ
 32 MB RAM SIMM
 Disco Rígido Western Digital 2.2GB
 Lectora de CD 8X (No Funciona Correctamente)
 Disketera 3 1/2 ''
 2MB Video Onboard
 Creative Soundblaster 16 (ISA)
 Modem 33600 US-Robotics
 Puertos ps/2 para teclado y mouse
 Puerto de RED Ethernet AT-1700 ONBOARD 10 Mbps (INTERFASE ROJA)
 Se agrego una placa de red PCI con chip RT-8139 (INTERFASE VERDE)
 También fue utilizado un MODEM ADSL marca Aresco en la practica pero este no será
 utilizado durante la demostración.

métodos de instalación

IP-COP permite su instalación mediante 3 métodos.

Method	Boot Floppy	Driver Floppy	CD Drive	FTP/Web Server
Bootable CD	N	N	Y	N
Bootable Floppy with CD	Y	N	Y	N
Bootable Floppy with FTP/Web Server	Y	Y	N	Y

En el primer metodo "Bootable CD" se bootea la PC por medio del CD y se instala el sistema operativo directamente desde en CD.

Este metodo es conveniente cuando se posee una PC con una lectora de CD que funciona correctamente y tiene la capacidad de booteo desde CD.

En el segundo metodo "Bootable Floppy with CD" Se inicia el sistema con un diskette y luego se inserta el CD para instalar el sistema operativo.

Este metodo es conveniente cuando se posee una PC con una lectora de CD que funciona correctamente y no se tiene la capacidad de booteo desde CD.

El método elegido por el grupo es "**Bootable Floppy with FTP/Web Server**" debido a que no funciona la lectora de CD y este es el único método que no la requiere.

En este método Se bootea con un diskette, se configura una interfase de red y se le proporciona al sistema una dirección URL de un servidor ftp conectado a la misma desde donde este copiara los archivos de instalación.

Tanto el cd como el diskette necesarios para la instalación se deben descargar previamente en formato de imagen ISO desde la pagina de IP-COP en Internet.

A continuación mostraremos brevemente como llevamos a cabo la instalación de IP-COP.

Instalación por el metodo Bootable Floppy with FTP/Web Server

Luego de insertar el diskette IP-COP en la diskettera se enciende el equipo.

Esto provoca que se active el LILO (**L**inux **L**oader) y se muestre la siguiente pantalla.

```

LILO

Welcome to IPCop, Licensed under GNU GPL version 2.

PLEASE BEWARE! This installation process will kill all
existing partitions on your PC or server. Please be aware
of this before continuing this installation.

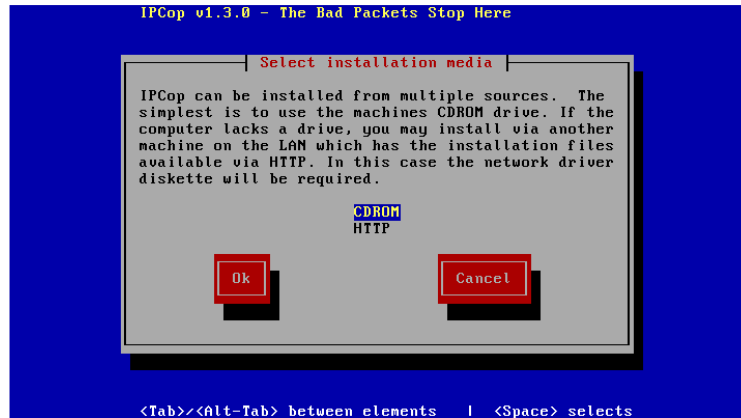
-----
---- ALL YOUR EXISTING DATA WILL BE DESTROYED ----
-----

Press RETURN to continue.

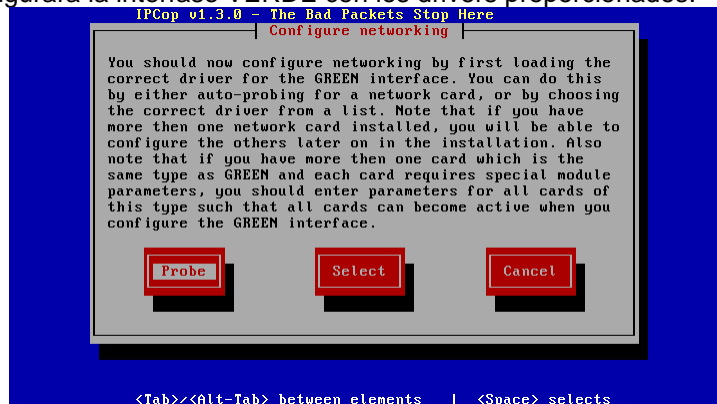
boot: _

```

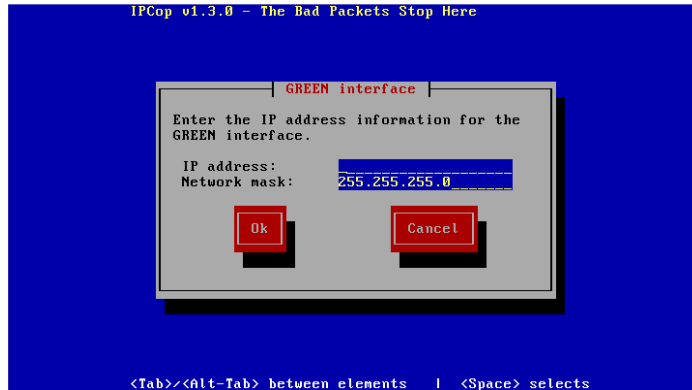
Esta pantalla es una advertencia de que la instalación eliminara todas las particiones existentes y se perderán todos los datos. Para continuar no pide presionar la tecla RETURN. Luego de confirmar nuestro deseo de instalar, el sistema corre el software instalador de ip-cop y nos pide que seleccionemos el idioma en el que se instalara. Luego de esto se nos da a elegir el método de instalación anteriormente mencionado.



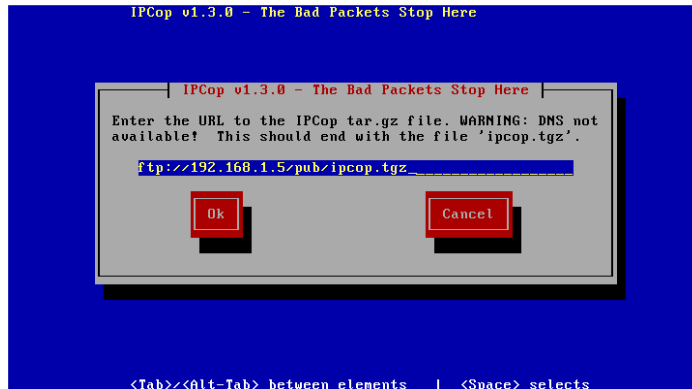
En nuestro caso se Eligio HTTP ya que no se posee una lectora de CD en operación. Ahora el sistema nos pedirá el driver floppy que es un diskette que se puede descargar así como los demás en la pagina oficial de ipcop. Este disco contiene los drivers de todas las placas que se especifican en la HCL de IP-COP. Previamente a la instalación hemos comprobado si nuestro hardware era compatible con la HCL del producto y verificamos que tanto la placa AT-1700 como al RT-8139 pertenecen dicha lista. La HCL de IP-COP esta disponible en la pagina oficial del producto en Internet. Una vez insertado el driver floppy continuamos con la instalación. El sistema configurara la interfase VERDE con los drivers proporcionados.



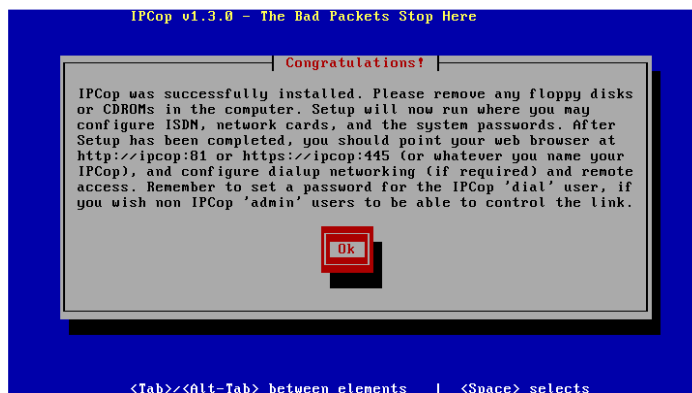
Una vez configurada la placa se nos solicita que le proporcionemos una dirección de IP y la correspondiente mascare de subred para dicha interfase del firewall, esta será la dirección con la que se vera al firewall desde la red interna de ahora en adelante.



Una vez suministrada la IP la interfase verde ya esta activa y configurada. Ahora el sistema nos solicitara la URL de el servidor desde donde se deben descargar los archivos de instalaci3n.



En nuestro caso se utilizo una PC Port3til con un Microsoft Internet Information Server instalado. Una vez que los archivos fueron descargados e instalados el sistema solicita que se extraigan los diskettes que pueda haber en la unidad de diskettes y pide una confirmaci3n para resetear el equipo. Una vez que la PC se reinicio se abre nuevamente el programa de instalaci3n que nos informa que la instalaci3n finalizo correctamente.



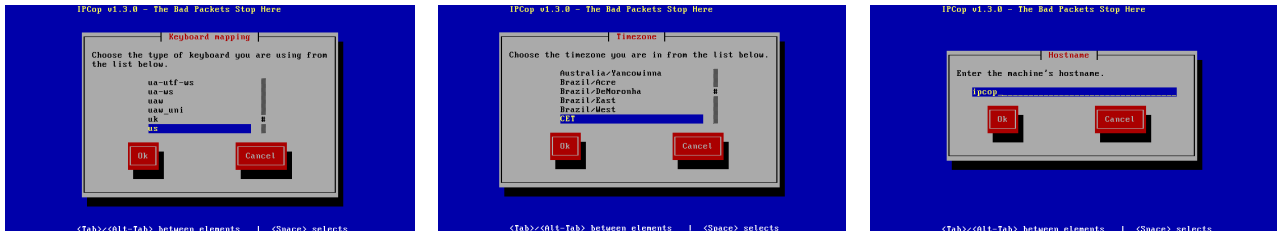
A partir de este momento el programa de instalaci3n abre el programa de configuraci3n inicial. (Aqui empieza el proceso de configuraci3n)

3.4. Configuraci3n

Durante esta sección se explicara como se realiza la configuración estándar de la distribución, en la primera parte se vera la configuración inicial que es la que se realiza en el momento posterior a la instalación, luego examinaremos la configuración vía web por medio de https y por ultimo mostraremos como se refleja esta configuración en los archivos de linux por medio de la consola.

Configuración inicial

Esta es la configuración que se realiza en el momento inmediatamente posterior al proceso de instalación del producto.

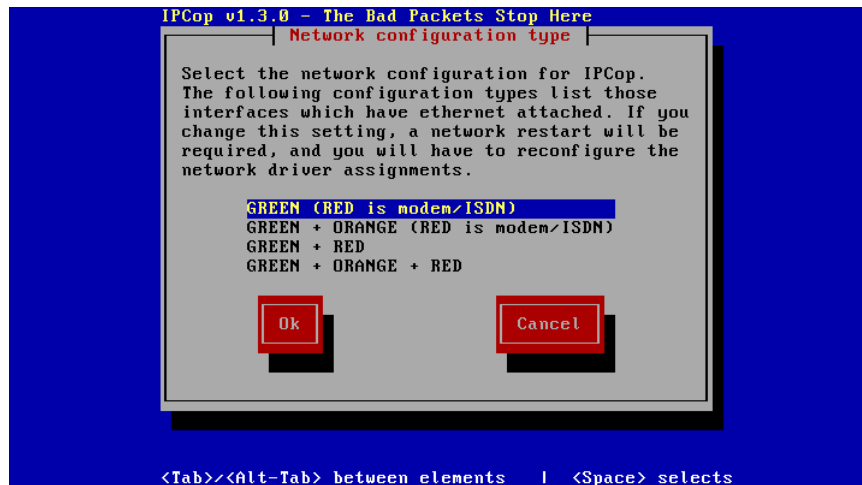


Las primeras pantallas nos solicitan información básica como la configuración del teclado, la zona horaria en donde nos encontramos, y el hostname.

A continuación se despliega la pantalla de configuración de ISDN. Esta pantalla no nos es de utilidad ya que no poseemos dispositivos ISDN.

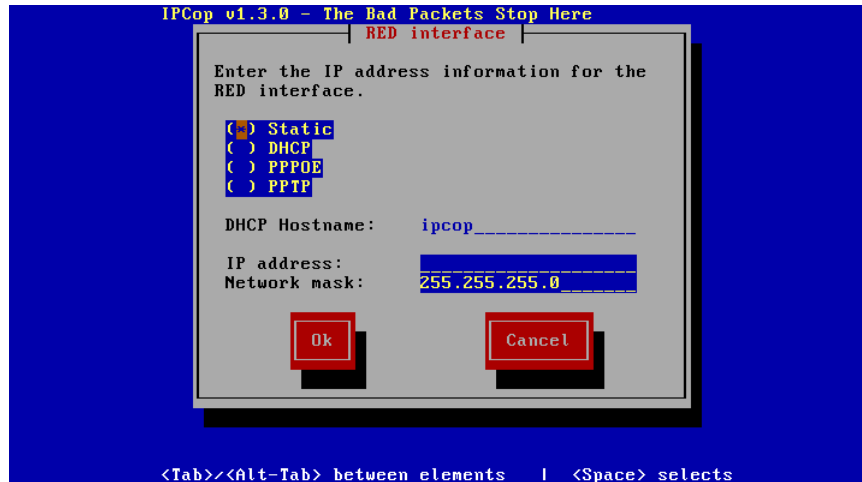
En el siguiente paso se muestra la pantalla que permite elegir el modo de instalación. Como ya hemos explicado en la sección 3.2 el firewall tiene cuatro modos de trabajo.

- GREEN (RED is modem/ISDN)
- GREEN + ORANGE (RED is modem/ISDN)
- GREEN + RED (RED is Ethernet)
- GREEN + ORANGE + RED (RED is Ethernet)



Elegimos el modo GREEN + RED (RED is Ethernet)

Luego de elegir el modo de trabajo pasamos a configurar la interfase ROJA(RED).

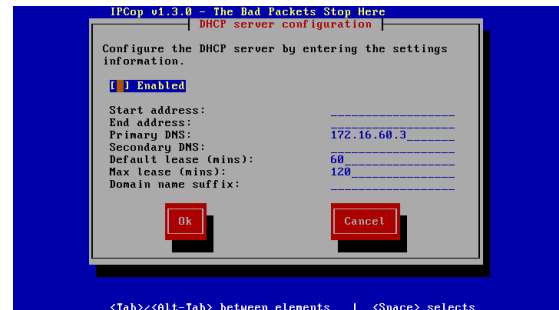
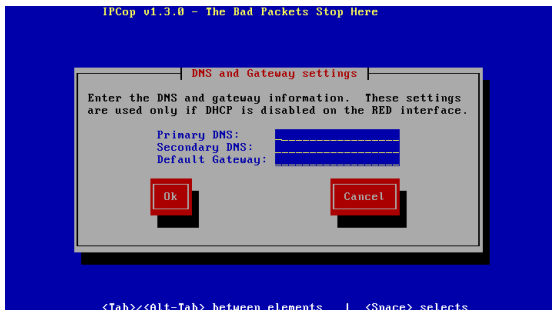


En esta pantalla se nos pide que ingresemos el medio por el cual se obtendrá la dirección ip desde la red considerada como peligrosa o que ingresemos una IP estática para dicha interfase.

En la practica que realizo el grupo se Eligio PPPOE ya que se trataba de una interfase ethernet conectada a un MODEM ADSL.

La dirección IP es entregada en forma dinámica por el ISP.

Luego se solicita la configuración del DNS del equipo y el DHCP Server.



Se solicitan los parámetros indispensables como DNS primario y secundario, y en el caso de el DHCP Server se pide el Scope de IP la mascara de subred el DNS primario y secundario y el sufijo de DNS para configurar en las estaciones de trabajo de la red VERDE.

Ahora se nos solicita que se ingresen las passwords para los 3 usuarios principales de la distribución:

Esta distribución genera automáticamente 3 usuarios para realizar las diferetes tareas de administración:

ROOT: Usuario utilizado para el acceso mediante la línea de comando.

SETUP: Usuario para acceder al programa de configuración.

ADMIN: Usuario para acceder vía HTTPS.

Aquí termina la Configuración inicial de IP-COP

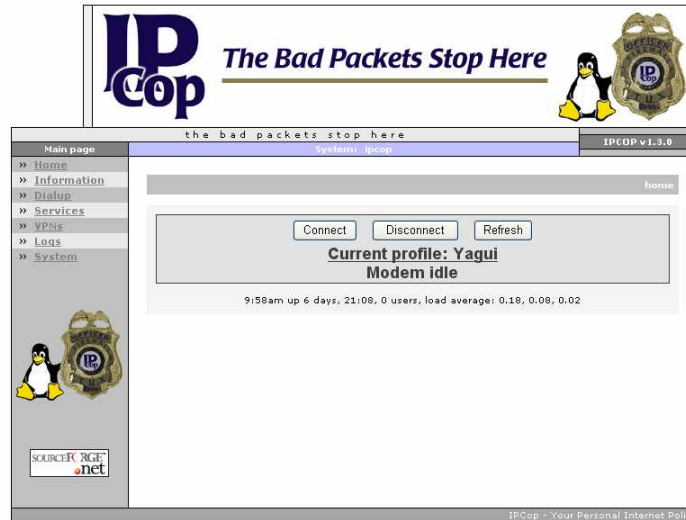
A partir de este momento el firewall ya puede verse desde la red interna lo único que falta para que este operativo es la configuración de algunos parámetros como el marcado del MODEM, etc.

Para configurar estos parámetros utilizaremos la administración vía web que ofrece la distribución por medio de HTTPS:

Configuración vía WEB

Desde una PC en la red interna se abre un Browser y se ingresa a la dirección de la interfase verde del firewall por medio del protocolo https en el puerto 445. En nuestro caso la dirección seria <https://192.168.1.1:445/>

Una vez que se despliega la pagina de administración nos aparece un menú con varias opciones.
Apenas se seleccione cualquiera de las opciones se nos solicitara un usuario y password para ingresar a la pagina, Este usuario determinara nuestro nivel de acceso.



El usuario que utilizaremos será admin. Ya que es el usuario que esta destinado a la administración web y ya esta configurado, luego se pueden configurar otros usuarios como por ejemplo "dial" que solo tiene permisos para conectar y desconectar el MODEM. Ahora procederemos a configurar la conexión con el MODEM. Aquí se mostrara como realizar la configuración básica para que el firewall quede operativo, las demás funciones de el acceso vía web serán explicadas en el punto 3.5 (Administración). Para realizar la configuración del MODEM nos dirigimos al menú **Dial Up** En este menú se pueden encontrar todas las opciones de configuración para los diferentes tipos de acceso.

The screenshot displays the IP-Cop web administration interface. At the top, it features the IP-Cop logo with the slogan "The Bad Packets Stop Here" and a penguin mascot. The main content area is titled "PPP setup" and contains several configuration sections:

- Profiles:** A dropdown menu shows "1_Yagui" selected, with "Select" and "Delete" buttons.
- Interface:** A dropdown menu shows "PPPoE" selected, with a "Refresh" button.
- Telephony:** Includes fields for "Maximum retries" (500), "Idle timeout (mins; 0 to disable)" (0), and checkboxes for "Persistent connection" (checked), "Dial on Demand" (unchecked), "Connect on IPCop restart" (checked), and "ISP requires Carriage Return" (checked).
- Additional PPPoE settings:** Fields for "Service name" and "Concentrator name", with a note: "This field may be blank."
- Authentication:** Fields for "Username" (cejago@speedy), "Password" (masked with dots), "Method" (PAP or CHAP), and "Script name".
- DNS:** Radio buttons for "Manual" and "Automatic" (selected), with fields for "Primary DNS" (200.51.254.254) and "Secondary DNS" (200.51.254.251).

At the bottom of the configuration area are "Save" and "Restore" buttons. The footer of the page reads "IP-Cop - Your Personal Internet Police".

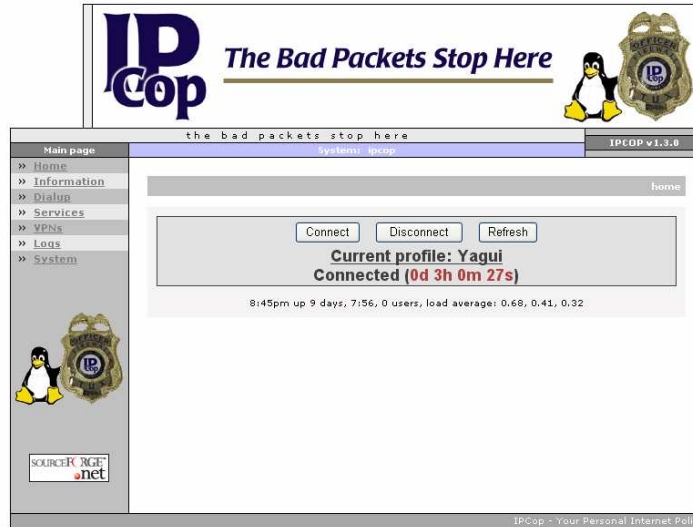
En esta pantalla se pueden configurar parámetros como el tipo de conexión, el nombre de usuario y passwords, la cantidad de reintentos y los servidores de DNS. Luego de ingresar estos datos ya se podrá conectar el firewall a Internet desde la página Home lo que lo dejaría en un estado operativo. El resto de la funcionalidad que ofrece la administración vía web será explicado en la sección 3.5 dedicada a Administración.

3.5. Administración

En esta sección mostraremos cómo se administra IP-COP de forma remota.

IP-COP permite su administración mediante SSH o HTTPS.

Este es un breve resumen de las opciones disponibles, solo mostraremos las opciones que el grupo utilizó para configurar el firewall, la explicación del resto de las funcionalidades se puede encontrar en la bibliografía sugerida.



La pagina de administración nos permite navegar entre 7 diferentes menús:

- Home
- Information
- Dial-Up
- Services
- VPNs
- Logs
- System

Home:

Es la pagina principal y es la que permite conectar y desconectar el firewall de Internet, esta es la única pagina a la que tiene acceso el usuario dial que es un usuario destinado solo para conectar y desconectar el firewall.

además esta es la pagina que le da acceso al administrador a todos los demás menús.

4. Test de penetración

En esta etapa se efectuaron ataques desde la red no segura hacia la red interna en la situación protegida y no protegida y se compararon sus resultados para determinar la eficacia del firewall.

4.1. Software Utilizado

El software que se utilizara para efectuar los ataques será el Shadow Security Scanner Reconocido como el mas rápido scanner de seguridad en el mercado actual, Shadow Security Scanner esta diseñado para identificar las vulnerabilidades conocidas y las aun no descubiertas, sugiere soluciones a las vulnerabilidades ya conocidas y reporta los posibles agujeros de seguridad en entornos de red, Internet, Intranet o extranet. La tecnología patentada de este producto eclipsa por completo las capacidades de las pasadas generaciones de scanners de seguridad y empleando un motor único de AI (inteligencia artificial) que permite al producto pensar como un hacker o un analista de seguridad de redes que intenta penetrar en la red interna.

Otras herramientas conocidas en el mercado son:

- Retina Security Scanner.
- Nessus (Bajo plataformas Linux)
- Languard Security Scanner
- Internet Security Scanner

4.2. Tipos de ataques realizados

Shadow Security Scanner incluye módulos de auditoria de vulnerabilidades para la mayoría de sistemas y servicios. Estos incluyen:

NetBIOS, HTTP, CGI y WinCGI, FTP, DNS, vulnerabilidades DoS, POP3, SMTP, LDAP, TCP/IP, UDP, Registro, Servicios, Usuarios y cuentas, vulnerabilidades en passwords, extensiones de publicación, MSSQL, IBM DB2, Oracle, MySQL, PostgreSQL, Interbase, MiniSQL, y muchos mas.

Shadow Security Scanner corre bajo Windows, pero su uso no esta limitado a esta plataforma, ya que como herramienta de red, permite scannear todo tipo de sistemas, incluyendo sistemas UNIX y dispositivos de red (routers, firewall, etc) que utilicen sistemas nativos.

4.3. Comparación (Situación protegida y no protegida)

Cuando realizamos el escaneo en la situación no protegida se detectaron puertos de utilizacion interna como 1521 (Oracle) y otros puertos que figuraban abiertos, además se detecto el nombre de la estación de trabajo los recursos compartidos , los Fix faltantes en el sistema operativo, y otras vulnerabilidades como el password de administrador en blanco. En la situación protegida lo único que se pudo detectar como puertos abiertos fueron el puerto 445 y el puerto 222 que son los utilizados para la administración remota de IP-COP y era lo que teniamos pensado que se detecte.

5. Solución de intrusión

En esta sección se mostrara como funciona el sistema de detección de intrusos que utiliza IP-COP.

El sistema utilizado es SNORT que es uno de los mas modernos y los mas utilizados en el mercado.

A continuación se describirá su clasificación , funcionamiento y cual es su potencial a la hora de detectar intentos de intrusión en nuestra red.

5.1. Detección de intrusos (SNORT)

Un IDS o Sistema de Detección de Intrusiones es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático o red informática en busca de intentos de comprometer la seguridad de dicho sistema.

Los IDS buscan patrones previamente definidos que impliquen cualquier tipo de actividad sospechosa o maliciosa sobre nuestra red o host.

Los IDS aportan a nuestra seguridad una capacidad de prevención y de alerta anticipada ante cualquier actividad sospechosa. No están diseñados para detener un ataque, aunque sí pueden generar ciertos tipos de respuesta ante éstos.

Los IDS: aumentan la seguridad de nuestro sistema, vigilan el tráfico de nuestra red, examinan los paquetes analizándolos en busca de datos sospechosos y detectan las primeras fases de cualquier ataque como pueden ser el análisis de nuestra red, barrido de puertos, etc.

Tipos de IDS

Según sus características



Pasivos

Son aquellos IDS que notifican a la autoridad competente o administrador de la red mediante el sistema que sea, alerta, etc. Pero no actúa sobre el ataque o atacante.

Activos

Generan algún tipo de respuesta sobre el sistema atacante o fuente de ataque como cerrar la conexión o enviar algún tipo de respuesta predefinida en nuestra configuración.

Snort puede funcionar de las dos maneras.

Arquitectura de IDS

- Normalmente la arquitectura de un IDS, a grandes rasgos, está formada:
La fuente de recogida de datos. Estas fuentes pueden ser un log, dispositivo de red, o como en el caso de los IDS basados en host, el propio sistema.
- Reglas que contienen los datos y patrones para detectar anomalías de seguridad en el sistema.
- Filtros que comparan los datos snifados de la red o de logs con los patrones almacenados en las reglas.
- Detectores de eventos anormales en el tráfico de red.
- Dispositivo generador de informes y alarmas. En algunos casos con la sofisticación suficiente como para enviar alertas vía mail, o SMS.
- Esto es a modo general. Ya veremos que cada IDS implementa la arquitectura de manera diferente.

Snort, por ejemplo, tiene una arquitectura dividida en tres subsistemas:

- Decodificador de paquetes
- Motor de detección
- Loggins y alertas

Evidentemente, son parte de la arquitectura global de un IDS que hemos comentado líneas más arriba.

Donde es conveniente colocar el IDS.

Una actitud paranoica por nuestra parte nos podría llevar a instalar un IDS en cada host ó en cada tramo de red. Esto último sería un tanto lógico cuando se trata de grandes redes. Lo lógico sería instalar el IDS en un dispositivo por donde pase todo el tráfico de red que nos interese.

Dificultades

Un problema de los IDS es cuando queremos implementarlos en redes commutadas ya que no hay segmento de red por donde pase todo el tráfico.

Otro problema para un IDS son las redes con velocidades de tráfico muy altas en las cuales es difícil procesar todos los paquetes.

Posición de IDS

Si colocamos el IDS antes del firewall capturaremos todo el tráfico de entrada y salida de nuestra red. La posibilidad de falsas alarmas es grande.

La colocación detrás del firewall monitorizará todo el tráfico que no sea detectado y parado por el firewall, por lo que será considerado como malicioso en un alto porcentaje de los casos . La posibilidad de falsas alarmas es muy inferior.

Algunos administradores de sistemas colocan dos IDS, uno delante y otro detrás del cortafuegos para obtener información exacta de los tipos de ataques que recibe nuestra red ya que si el cortafuegos está bien configurado puede parar o filtrar muchos ataques.

En ambientes domésticos, que es el propósito de este trabajo, podemos colocar el IDS en la misma máquina que el firewall. En este caso actúan en paralelo, es decir, el firewall detecta los paquetes y el IDS los analiza.

Introducción a SNORT

Snort es un IDS o Sistema de detección de intrusiones basado en red (NIDS). Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, intentos aprovechar alguna vulnerabilidad, análisis de protocolos, etc conocidos. Todo esto en tiempo real.

Snort (www.snort.org) está disponible bajo licencia GPL, gratuito y funciona bajo plataformas Windows y UNIX/Linux. Es uno de los más usados y dispone de una gran cantidad de filtros

o patrones ya predefinidos, así como actualizaciones constantes ante casos de ataques, barridos o vulnerabilidades que vayan siendo detectadas a través de los distintos boletines de seguridad.

Este IDS implementa un lenguaje de creación de reglas flexible, potente y sencillo. Durante su instalación ya nos provee de cientos de filtros o reglas para backdoor, ddos, finger, ftp, ataques web, CGI, escaneos Nmap....

Puede funcionar como sniffer (podemos ver en consola y en tiempo real qué ocurre en nuestra red, todo nuestro tráfico), registro de paquetes (permite guardar en un archivo los logs para su posterior análisis, un análisis offline) o como un IDS normal (en este caso NIDS).

La colocación de Snort en nuestra red puede realizarse según el tráfico

Es posible vigilar: paquetes que entran, paquetes salientes, dentro del firewall, fuera del firewall... y en realidad prácticamente donde queramos.

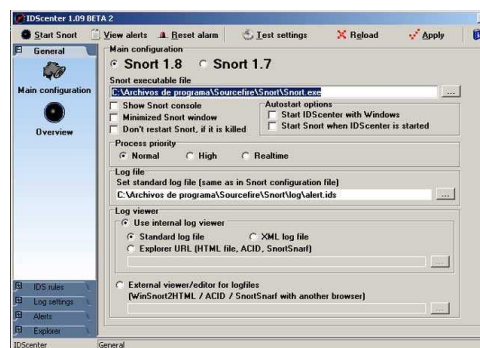
Una característica muy importante e implementada desde hace pocas versiones es FlexResp. Permite, dada una conexión que emita tráfico malicioso, darla de baja, hacerle un DROP mediante el envío de un paquete con el flag RST activa, con lo cual cumpliría funciones de firewall, cortando las conexiones que cumplan ciertas reglas predefinidas. No sólo corta la conexiones ya que puede realizar otras muchas acciones. Veremos más adelante su funcionamiento y ejemplos.

Formato de la cabecera (header) del TCP



Snort como sniffer se basa en las librerías de captura de paquetes libcap que provee a snort de la capacidad de sniffer de paquetes. En windows la librería sería WinPCAP.

Snort puede, para su fácil configuración y gestión, usarse mediante una interfaz gráfica. Por Ejemplo IDSCenter.



IDSCenter, ahora en su versión 1.09 Beta 2, es una internase gráfica que nos sirve para configurar todas las características de Snort como las alertas, tests, reglas, variables,

funcionamiento junto a MySQL o BlackIce Defender, rotación de logs, notificaciones via mail o sonido, plugins, preprocesadores, FlexResp ...

5.2. Tipos de ataques detectados

El Archivo Alert.ids es el archivo donde se almacenarán las alertas y registros de paquetes generados por Snort. Tiene un formato ASCII plano, fácilmente editable por cualquier procesador de textos.

Alert.ids está ubicado en el directorio /log dentro de la carpeta donde se realizó la instalación.

*En este directorio también se almacenarán otros Archivos, como los relacionados a salidas o registros del preprocesador de scan de puertos o los registros de alertas asociados a la dirección IP que generó la alerta.

Para mejor comprensión de las alertas generadas por Snort, podemos configurar desde IDSCenter dos tipos de alertas:

Set alert mode FAST o Alerta Rápida

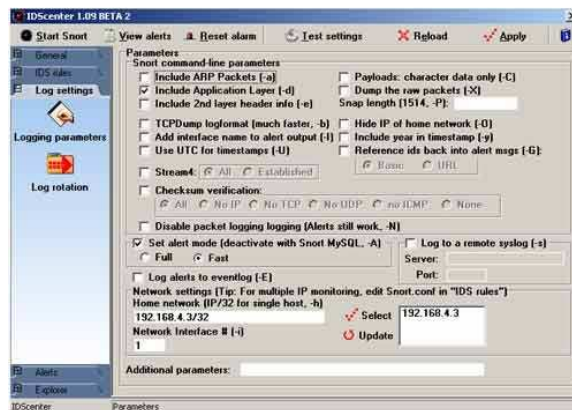
Set alert mode FULL o Alerta Completa

El modo Alerta Rápida nos devolverá información sobre: tiempo, mensaje de la alerta, clasificación, prioridad de la alerta, IP y puerto de origen y destino.

El modo de Alerta Completa nos devolverá información sobre: tiempo, mensaje de la alerta, clasificación, prioridad de la alerta, IP y puerto de origen/destino e información completa de las cabeceras de los paquetes registrados.

Para configurar estos dos modos en IDSCenter:

Panel Log setting > Logging parameters



Marcamos en "Set alert mode (desactivate with Snort MySQL...)" y a continuación entre Full y Fast. Terminada la operación Aplicamos la regla ("Apply") y "Start Snort".

Veamos dos ejemplos:

Se trata de dos simples accesos a un servidor Proxy ubicado en el puerto 8080 de la máquina destino IP: 192.168.4.15 por parte del host IP: 192.168.4.3 que realiza la conexión mediante el puerto 1382 en el primer caso y 3159 en el segundo.

Snort clasifica o describe esta alerta como un intento de pérdida de información, clasificado como prioridad 2.

Modo Alerta Rápida:

```
09/19-19:06:37.421286 [**] [1:620:2] SCAN Proxy (8080) attempt [**]
```

```
[Classification: Attempted Information Leak] [Priority: 2] ...
```

```
... {TCP} 192.168.4.3:1382 -> 192.168.4.15:8080
```

Modo Alerta Completa:

```
[**] [1:620:2] SCAN Proxy (8080) attempt [**]
```

```
[Classification: Attempted Information Leak] [Priority: 2]
```

```
09/19-14:53:38.481065 192.168.4.3:3159 -> 192.168.4.15:8080
```

```
TCP TTL:128 TOS:0x0 ID:39918 IpLen:20 DgmLen:48 DF
```

```
*****S* Seq: 0xE87CBBAD Ack: 0x0 Win: 0x4000 TcpLen: 28
```

```
TCP Options (4) => MSS: 1456 NOP NOP SackOK
```

Información de la cabecera del paquete:

TCP TTL:128 TOS:0x0 ID:39918 IpLen:20 DgmLen:48 DF
*****S* Seq: 0xE87CBBAD Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1456 NOP NOP SackOK

5.3. Comparación (Situación protegida y no protegida)

Podemos notar que en la situación desprotegida una persona que estuviese en el exterior de nuestra red podría detectar las vulnerabilidades que teníamos fácilmente y explotarlas con fines maliciosos sin ser detectada por nuestra red.

En la situación protegida , no solo no se pudieron detectar las vulnerabilidades que hay detrás del firewall sino que además se eliminaron dichas vulnerabilidades y se detectaron por medio del IDS todos los ataques realizados.

6. Conclusiones

Creemos que IP-COP puede ser una muy buena solución para particulares o pequeñas empresas que requieran una eficaz protección de su red y no dispongan de un gran presupuesto, con este producto de licencia gratuita se puede reciclar hardware obsoleto y tener un sistema confiable que además puede utilizarse como Proxy, DHCP y hasta permite la comunicación por medio de VPN que podría ser útil para intercambiar datos entre sucursales.

además hay que tener en cuenta que últimamente el mercado tiene una gran tendencia hacia el Software Abierto, y creemos que esta tendencia seguirá creciendo ya que entre otras ventajas es mucho mas económico que el software cerrado.

7. Bibliografía

<http://www.snort.org/>
<http://www.netfilter.org/>
<http://www.ipcop.org/>
<http://www.safety-lab.com/en/products/1.htm>
<http://www.linux.org.ar/>



Javier Ordoñez Ojeda
achalay@movi.com.ar
Fernando Gabriel Camisar
Andres Alfredo Berner
Mariano Crimmi
Esteban Darreche
Pablo Jaca

Buenos Aires. Argentina