MANUAL DE SEGURIDAD INFORMATICA AYSATEC S.A.S PROTECCION CONTRA INTRUSOS:

AYSATEC SAS utiliza un sistema de firewall basado en RouterOS Mikrotik para protegerse de las Botnets, así como de cualquier intruso o tercero con intenciones de vulnerar la seguridad, no solo los Equipos instalados en la cabecera sino también la información de nuestros usuarios, cabe destacar que las Botnet puede controlar todos los ordenadores/servidores infectados de forma remota) son, hoy en día, los sistemas más complejos y peligrosos en el mundo informático. Sus objetivos, además de las grandes empresas, son los usuarios domésticos de los proveedores de internet. Tienen protocolos preferidos para el ataque, como Telnet, NTP, SSH; esta es una pequeña lista de los protocolos que preferentemente suelen atacar;

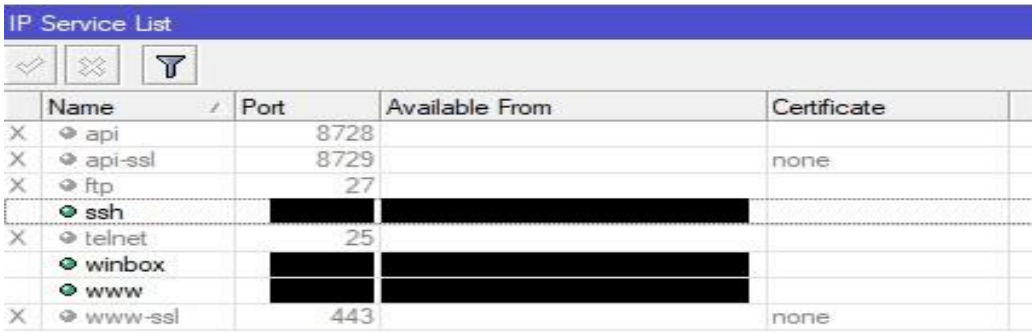
FTP (TCP/20,21) SSH (TCP/22) Telnet (TCP/23,2323) DNS (UDP/53) TFTP (TCP/69) HTTP (TCP/80,8080,8880) NTP (UDP/123) POP3 (TCP/110,995) IMAP (TCP/143,220,993)

HTTPS (TCP/443) RDP (TCP/3389) SMTP (TCP/25,465,587) Winbox (TCP/8291) VNC (TCP/5500,5800,5900)

Estos protocolos están supervisados y debidamente restringidos en la red a través de nuestro firewall, el cual discrimina no solo la ip de conexión sino también la cantidad de accesos, generando un accseslist con nombre “Blacklist” la cual banea la IP remota de conexión.

A través de dicha lista de acceso “Blacklist” se realiza un bloqueo de L3 de subredes listadas como SPAM, servidores madre de Command & Control y de Botnets conocidos a nivel mundial.

Aunado a este esfuerzo, realizamos cambio en los puertos de los protocolos de administración críticos en el equipo de borde y deshabilitamos completamente los que no son necesarios. La combinación de todas estas acciones genera una muy difícil tarea para lograr ingresar o controlar nuestros equipos de borde, sin la debida autorización y el conocimiento.



Avenida 52 # 21-76 Barrio Colorados
Celular: 3183637018
Correo: aysatec@gmail.com

A continuación, las acciones más importantes implementadas en nuestros equipos para prevención de intrusos:
Las fases de un ataque informático son las siguientes:

Reconocimiento:

En este ITEM el atacante utiliza diferentes métodos para obtener información de la red o del objetivo, tomando en cuenta esto, constantemente se educa al personal de no Revelar datos confidenciales y ser cuidadosos al momento de almacenar datos importantes los cuales podrían abrir una puerta a posibles ataques.

Exploración:

Con base a la información recolectada el atacante, verifica los exploits y vulnerabilidades que le permitan obtener acceso y violar la seguridad, para ello realizamos un bloqueo de escaneo de puertos en nuestro equipo de Borde y constantemente realizamos actualizaciones de software del mismo.
Con el siguiente script se analiza automáticamente si una IP se encuentra realizando mapeo de puertos y dropea dichos paquetes.
/ip firewall filter
add chain=input protocol=tcp psd=21,3s,3,1 action=add-src-to-address-list addresslist="port scanners" address-list-timeout=2w comment="Port scanners to list " disabled=no
add chain=input src-address- list=port-scanners action=drop

Obtener acceso:

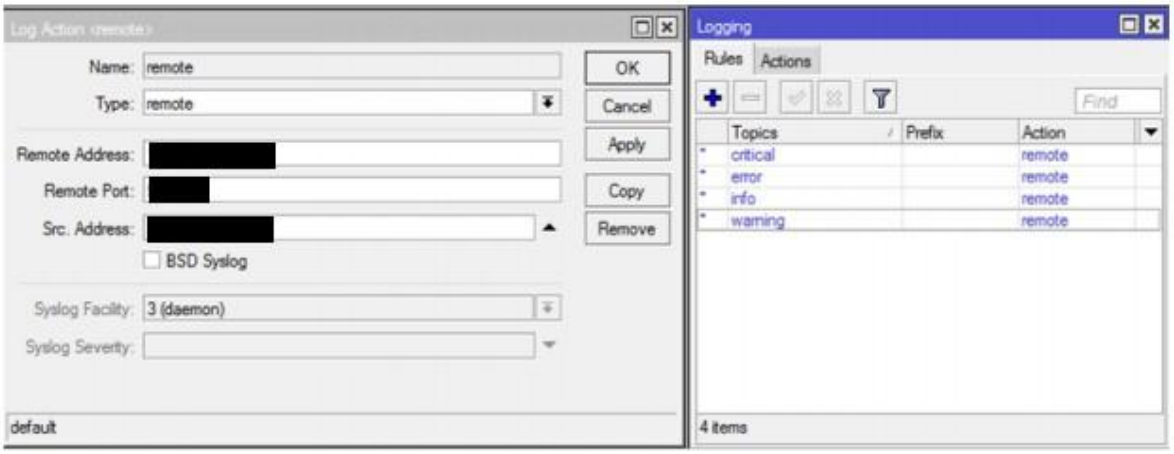
El atacante, utiliza las vulnerabilidades encontradas y a través de sistemas operativos como (Kali Linux) y métodos de Buffer Overflows, DDoS, Session Hijacking o Password Cracking, para lograr el acceso a los sistemas y tomar control del mismo. Para ellos establecemos políticas de control y filtrado, lo que garantiza la identidad y los privilegios de cada conexión.
BLOQUEO DoS:
/ip firewall filter add chain=input
protocol=tcp connection-limit=10,32 action=add-src-to-address-list addresslist=blocked-addr address-list-timeout=1d
/ip firewall filter add chain=input
protocol=tcp src-address-list=blocked-addr connection-limit=3,32 action=tarpit
BLOQUEO SYN Flood:

/ip firewall filter add chain=forward protocol=tcp tcp-flags=syn connection-state=new action=jump jump-target=SYN-Protect comment="SYN Flood protect" disabled=no
/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn limit=400,5 connection-state=new action=accept comment="" disabled=no

/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn connectionstate=new action=drop disabled=no
/ip settings set tcp-syncookies=yes
En nuestro Firewall activamos el bloqueo de puerto 53UDP, esta acción se previene un tipo de ataque muy común de DDoS (denegación de servicio), el cual tiene la finalidad de enviar solicitudes a posibles servidores DNS dentro de la red saturando el enlace con solicitares falsas.
Esta implementado en el Equipo de Borde de la siguiente manera:
/ip firewall filter add action=drop chain=input disabled=no dst-port=53 ininterface=WAN protocol=udp Mantener Acceso.

El atacante genera una puerta trasera oculta, instalando trojans o scripts, las actualizaciones periódicas previene que se puedan utilizar los exploits de versiones antiguas en instalar este tipo de aplicativos dentro del equipo lo que le permita tener un control discreto del mismo.
 Borrar Huellas.

En este ítem se borras los rastros de acceso al equipo eliminando los logs, para ello se habilita un servidos SysLog centralizado al cual se envían todos los registros y protegerlo de accesos no autorizados.



SEGURIDAD DE LA INFORMACIÓN:

Avenida 52 # 21-76 Barrio Colorados
Celular: 3183637018
Correo: aysatec@gmail.com

AYSATEC SAS comprometida con sus usuarios y la seguridad de la información implementa un conjunto de medidas preventivas y reactivas, que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

PRIVACIDAD DE LA RED:
Para considerar una red como segura debe garantizar las siguientes características: Disponibilidad, autenticación, integridad y confidencialidad.

POLÍTICA DE SEGURIDAD:
INFRAESTRUCTURA
Red Principal
Instalación de Firewall, cuya función es separa los segmentos de redes internos y los externos colocando restricciones a conexiones no autorizadas.
Verificación periódica de los Logs del sistema Firewall

Red Domestica
Restringir las conexiones Usuario a Usuario.
Activación de firewall al modem, utilizar modos de autenticación fuertes para las redes Wifi con WPA2-AES.

Orientar al usuario de los diferentes peligros que existen en la red sobre Ciberdelitos y fraudes y que puede hacer para protegerse, como la utilización de Firewalls, Antivirus y Antimalware en sus dispositivos.

POLITICAS GENERALES
Como objetivo adicional del proyecto se decidió la creación de una política de seguridad en la que enmarcar el sistema.

Implementación
Los procesos de logging de las aplicaciones y los sistemas operativos deben estar activados en todos los módems y servidores.
Las funciones de alarma y alerta de los firewalls y otros dispositivos de control de acceso al perímetro deben estar activos.

Administración Se deben revisar diariamente los logs en los sistemas de control de acceso al perímetro (firewall).
Se deben revisar semanalmente los logs de los hosts y servidores que se encuentran en la red interna.
Se debe entrenar a los usuarios para que avisen de cualquier anomalía en el rendimiento del sistema a los administradores.
Todos los problemas que reciban los administradores serán revisados en busca de síntomas que indiquen actividad intrusa.
Los síntomas sospechosos deberán ser comunicados a los administradores de la RED.

Cuando se produzca una intrusión, a menos que los sistemas críticos hayan sido comprometidos, la organización intentará primero recabar pruebas sobre los intrusos antes de reparar los sistemas, buscando más información de quién y cómo se produjo la intrusión. Esta persona debe ser entrenada en las vías legales para reportar una intrusión.

Se permitirá que determinados agujeros de seguridad queden sin corregir controladamente para el estudio de los atacantes y sus técnicas (’honeypots’).

Antivirus

La protección contra virus debe realizarse en dos frentes:
- Correo electrónico de los clientes del ISP
- Usuarios internos de un ISP (Personal administrativo)

Correo electrónico de clientes

Uno de los servicios más usados por los clientes de un ISP es el correo electrónico. El intercambio de archivo de correo es elevado y constante. En este sentido Cable Éxito bloquea las subredes bien conocidas y enlistadas como SPAN

Alcance
Para la revisión de los virus en los archivos de correo se debe de instalar un software antivirus y mantenerlo constante actualizado.

Objetivos
Filtrar los correos que contengan virus y SPAN que puedan infectar los equipos de los clientes.

Elementos
El principal elemento es el software antivirus que debe estar constantemente actualizado.

Responsabilidades
Para ellos e concientiza al usuario el uso y actualización de dicho software.

USUARIOS INTERNOS

Alcance:
Proteger a cada uno de los equipos de la red interna del ataque de virus informáticos.

Objetivos:
Prevenir de infecciones de virus informáticos en la red interna.

Elementos/Recursos:
El principal elemento es el software antivirus que debe estar constantemente actualizado y el personal que labora en la empresa.

Responsabilidades:

El administrador de sistemas es la persona encargada de la actualización del software antivirus cada 15 días para que este pueda detectar las más recientes modificaciones de los virus.
Chequear los CD-ROM's ingresados en nuestra PC sólo una vez, esto no aplica si son regrabables.
Revisar toda memoria USB que provenga del exterior, es decir que no haya estado bajo nuestro control. Aún cuando nos indiquen que está revisado. Nunca sabemos si esa persona sabe operar correctamente su antivirus.
Al bajar páginas de Internet, archivos ejecutables, etc. Estos siempre deben ser revisados antes de ejecutarlos. Y la descarga debería ser realizada a un directorio específico, para luego de revisarlos pasarlos a las carpetas de trabajo.
Revisar todos los e-mails antes de abrirlos. Si llegan con un remitente desconocido, o archivos adjuntos que no conocemos de que se trata, eliminarlos inmediatamente. Antes de actualizar el antivirus, verificar nuestra PC completamente.

Medidas de Protección Efectivas
La mejor medida de protección es adquirir un antivirus y mantenerlo siempre actualizado. Adicionalmente mantenerse informado sobre las nuevas técnicas de ataques y como evitarlas. Actualmente existes muchos sitios de información sobre nuevos ataques y herramientas que nos protegen en línea.

Referencia para Software de Antivirus
Tener varios programas antivirus, preferentemente con diferentes enfoques.

- Utilizar o activar las diversas opciones de protección. Estas podrían ser: equipos personales, para servidores de Correo.
- Comprar las versiones actualizadas de las vacunas.
- Leer la documentación y manuales de los antivirus.

Avenida 52 # 21-76 Barrio Colorados
Celular: 3183637018
Correo: aysatec@gmail.com