INTRODUCCION A LA SEGURIDAD DE LA INFORMACION

INSTITUTO TECNOLOGICO DE MORELIA

Reporte Firewall

Carlos Sebastian Madrigal Rodriguez

18121699

Ingeniería en Tecnologías de la Información y la Comunicación

Prof. Antolino Hernández Anastacio

Departamento de Sistemas

Actividad 1. Basándose en los términos utilizados en el documento llamado "Firewall IPTables.doc", busque y defina:

1. **Qué entiende por un firewall de capa de red y un firewall en capa de aplicación, y cuál sería la diferencia en cuanto a facilidad de configuración.**
   Es dispositivo físico o software que filtra el tráfico entre redes, como mínimo dos.
2. **Las capas del modelo TCP/IP ¿qué capas comprende del modelo OSI?**
   - Acceso a la red -> Capa física y enlace.
   - Internet -> Capa de red.
   - Transporte -> Capa de transporte.
   - Aplicación -> Capa de sesión, presentación y aplicación.
3. **¿Qué se entiende por una red DMZ y qué servicios se instalan en ella?**
   Es una red o parte de una red separada de otros sistemas por un firewall, que permite que sólo entre o salga cierto tipo de tráfico de red. Los servidores web públicos, de correo y de dominios son algunos ejemplos de los servicios que se pueden instalar en una red DMZ.
4. **¿Qué se entiende por NAT (Network Address Translation), así como DNAT y SNAT?**
   Es un método de mapear o intercambiar un espacio de direcciones a otro, En caso de SNAT, El dispositivo que realiza NAT cambia la dirección IP privada del host de origen a una dirección IP pública, al contrario, DNAT cambia la dirección de destino en el encabezado IP de un paquete.
5. **Defina el concepto y funciones de un IDS (Intrusion Detection System), un IPS (Intrusion Prevention System) y un IRS (Intrusion Response System).**
   - IDS es un programa de detección de accesos no autorizados a un computador o a una red. Este sistema detecta, gracias a sensores virtuales, las anomalías que pueden ser indicio de la presencia de ataques y falsas alarmas.
   - IPS: Es una forma de seguridad de la red que trabaja en detectar y prevenir amenazas, este sistema monitorea la red de forma continua en busca de incidentes maliciosos y capturando información acerca de ellos, reportándolos al administrador del sistema.
   - IRS: Es un IDS que genera una respuesta proactiva para detener los ataques antes de que estos mismos ocurran, los IRS están continuamente monitoreando el estado de salud del sistema para aplicar medidas en contra para identificar y responder a incidentes potenciales.
6. **Defina qué entiende por firmas o patrones de ataque utilizado contra los sistemas informáticos.**
   Los patrones de ataque son ataques ya conocidos y preconfigurados usados como punto de comparación en un IPS. Este identifica el tipo de amenaza a ataque gracias a coincidencias o similitudes de ataques previos, a cada patrón de ataque se le conocen como firmas.
7. **¿Qué es el sistema SNORT y qué actividad o función realiza junto al firewall?**
   Es un sniffer de paquetes (capturador de tramas circulantes en la red) y un detector de intrusos. Basado en red, este provee de una base de datos de ataques la cual puede ser

usado a través de los diferentes módulos de firewall para detectar un posible ataque o compromiso a la seguridad. Este programa monitorea en tiempo real el trafico de la red, así como capacidad de generar archivos de registro.

Ahora, basándose en el documento llamado “Firewall IPTables.doc”, defina:

1. **¿Cuál es la dirección de la red local (LAN) en el diseño del firewall?**
   10.2.1.0/24, de las cuales, solo el rango de 10.2.1.1 a 10.2.1.200 serán expedidas por el servicio de DHCP.
2. **¿Cuál es la dirección IP utilizada para salir a Internet (WAN) en el diseño del firewall?**
   La última dirección utilizable de la subred: 10.2.1.254 (Gateway predeterminado).
3. **¿Cuál es la dirección IP del servidor que proporciona información pública (DMZ) en el diseño del firewall?**
   La IP 10.3.0.1 con mascara /24.
4. **¿Cuántas interfaces o tarjetas de red tiene el firewall, y cómo se identifican o se nombran esas interfaces?**
   Tiene 3 tarjetas de red físicas o interfaces identificadas por los nombres: Eth0, Eth1, Eth2 y una interfaz virtual lo (loopback) que hace referencia al propio sistema.
5. **Por último, describa el funcionamiento del firewall entre las redes conectadas a sus interfaces. Es decir, describa a grandes rasgos lo que realiza el firewall entre las redes que interconecta.**
   Realiza un escaneo de los servicios o puertos, así como el trafico expedido por las 2 computadoras conectadas directamente conectadas al firewall así como el trafico entrante y saliente a internet, en caso de que algún paquete que cumpla con alguna de las reglas impuestas en el firewall independientemente si sea malicioso o no, el firewall no le permitirá llegar a su destino o salir de la red.