Ejercicios Modulo 2 - Unidad 2

Alumno: Rodrigo Vila

Ejercicio Número 1 Unidad 2

A- ¿Si tuviéramos a nuestra disposición un servidor DNS, cuales piensan que serían los puntos a tener en cuenta en su creación respecto a la seguridad?

Para crear un servidor DNS con un enfoque sólido en la seguridad, sería importante considerar los siguientes puntos:

- **Actualizaciones regulares y parches de seguridad:** Mantener el servidor DNS actualizado con los últimos parches de seguridad es crucial para mitigar vulnerabilidades conocidas.
- **Configuración adecuada de permisos:** Asegurarse de que solo los usuarios autorizados tengan acceso de escritura a los datos DNS para prevenir la modificación no autorizada de los registros.
- **Implementación de autenticación y autorización:** Utilizar mecanismos de autenticación sólidos para controlar quién tiene acceso al servidor DNS y qué acciones pueden realizar.
- **Filtrado de consultas maliciosas:** Configurar el servidor DNS para filtrar y bloquear consultas sospechosas o maliciosas que puedan ser indicativas de intentos de ataque.
- **Monitoreo constante:** Establecer sistemas de monitoreo para detectar y responder rápidamente a cualquier actividad inusual o intentos de ataque.
- **Uso de firmas DNSSEC:** Implementar DNS Security Extensions (DNSSEC) para proteger contra la suplantación y la manipulación de datos DNS.
- **Limitación de consultas recursivas:** Configurar el servidor DNS para limitar las consultas recursivas solo a clientes confiables y autorizados, evitando así posibles ataques de denegación de servicio.
- **Segregación de funciones:** Separar el servidor DNS de otros servicios y limitar sus interacciones con otros componentes de la red para reducir la superficie de ataque.
- **Registro y análisis de eventos:** Llevar un registro detallado de todas las actividades del servidor DNS y realizar análisis periódicos para identificar posibles anomalías o intrusiones.

Al considerar estos puntos y adoptar un enfoque proactivo hacia la seguridad, se puede fortalecer significativamente la infraestructura de DNS y reducir el riesgo de compromisos de seguridad.

B- ¿En nuestro entorno de trabajo, en caso de disponer un servidor de DNS o DHCP, que sabemos de ellos?

Para ser sincero, nunca administré servidores que sean exclusivos para los servicios DNS o DHCP. Pero si he interactuado con estos servicios a través de mis servidores en su mayoria multi-propósito.

Mi experiencia con **DHCP** fue siempre a través de la configuración de las herramientas que proporciona un router, para que éste mismo se encarge de la administración del servicio. Del lado "cliente" sólo he configurado en el sector TCP/IP si el equipo recibe una dirección IP de manera automática (para que pueda auto-asignarse la IP administrada por el DHCP) o si va a llevar una configuración de IP fija, (en las mismas propiedades del protocolo TCP/IP).

En el caso del servicio **DNS**, a partir de la configuración que me proporciona mi proveedor de dominios, he configurado los registros para diversas tareas. Para direccionar, redireccionar, entregar informacion relevante, crear subdominios y hasta como método de autentificación de certificados SSL.

Tambien en servidores web como IIS y Apache he utilizado DNS para alojar múltiples sitios y redireccionar segun el DNS correspondiente a distintas ubicaciones/directorios dentro de la misma IP (virtual hosts).

A veces, para economizar gastos o según disponibilidad, he utilizado el servicio NO-IP, para enrutar un DNS específico hacia direcciones IPs dinámicas.

Por lo tanto, el primer contacto que tengo con servidores DNS o DHCP exclusivos es a través de ésta cursada.

También se puede utilizar DNS sin necesidad de internet. Asignando nombres de dominios a los equipos de una red LAN por ejemplo y asi poder establecer comunicación entre los dispositivos de la red utilizando sus nombres de dominio (o subdominios) en vez de sus direcciones IP.

C- De los distintos balanceadores de carga que vimos, ¿cuál sería el más conveniente para nuestra empresa y porque? (justificar la respuesta)

Para empezar quiero mencionar que seleccionaria un balanceo de carga entre firewalls (ya que esta cursada se trata de la seguridad de la informacion, es lo que voy a priorizar) para evitar que se sobrecargue uno de los filtros mas importantes que tenemos en nuestra hipotetica red.

Como método de balanceo de carga entre servidores, de los que vimos en éste módulo, el que me pareció mas conveniente es el método **"Nodo de balanceo"**. Ya que los clientes acceden

mediante este único nodo y éste se encarga de dirigir el tráfico a cualquiera de los nodos disponibles teniendo en cuenta las siguientes ventajas (cito):

"– Puede actuar como firewall.

– Puede asignar cargas de trabajo asimétricas, de manera que algunos nodos reciban más o menos peticiones en función de sus capacidades.

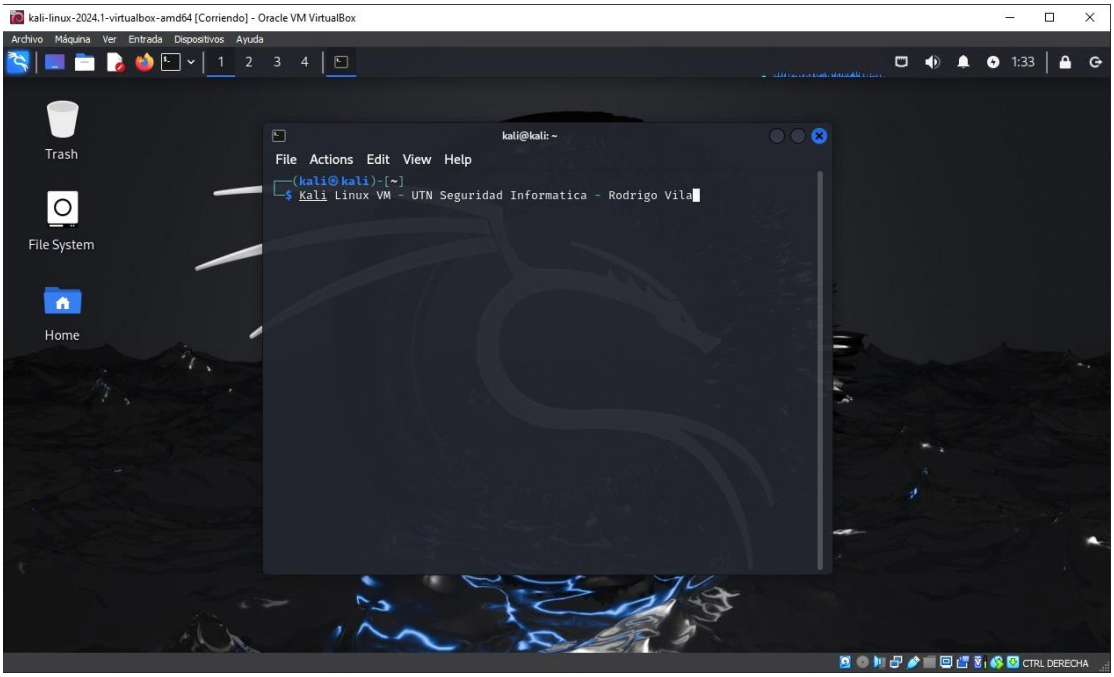
– Tiene tolerancia a fallos de los nodos servidores.

– Se puede realizar monitorización del estado en que se encuentran los nodos servidores.

– Se puede considerar una infraestructura clúster."

Tema adicional: Instalando Linux

Kali Linux corriendo en Virtual Box:



Rodrigo Vila.-