Servidores DNS

Capítulo destinado a contramedidas para solucionar vulnerabilidades en servidores de nombres de dominio.

- Resolución abierta de DNS
- Deshabilitar transferencia de zona

Resolución abierta de DNS

La vulnerabilidad Open Resolver DNS es una vulnerabilidad de seguridad que se refiere a los servidores de nombres de dominio (DNS) que han sido configurados de manera que permiten que cualquier persona en Internet realice consultas a través de ellos sin restricciones. Esto significa que un atacante puede enviar solicitudes de consulta DNS a estos servidores en grandes cantidades y utilizarlos como amplificadores en ataques de denegación de servicio distribuido (DDoS) contra otros sistemas en Internet.

En un ataque de DDoS que utiliza la vulnerabilidad Open Resolver DNS, el atacante envía una gran cantidad de solicitudes de consulta DNS falsas a los servidores Open Resolver, y éstos responden a estas solicitudes enviando grandes cantidades de datos a las direcciones de origen de las solicitudes. Al enviar muchas solicitudes falsas desde diferentes direcciones, el atacante puede hacer que los servidores de destino se vean abrumados por el tráfico de red y se vuelvan inaccesibles.

Para evitar la vulnerabilidad Open Resolver DNS, es importante que los administradores de sistemas configuren sus servidores DNS correctamente. Esto incluye restringir el acceso a los servidores de DNS, implementar listas de control de acceso (ACL), limitar el tamaño de los registros de consulta DNS, y actualizar el software de DNS regularmente para corregir vulnerabilidades conocidas.

Configuración DNS en Bind9

Agregue lo siguiente a las opciones globales:

Las opciones globales de BIND9 se definen en el archivo de configuración principal de BIND9, que normalmente se llama `named.conf` o `named.conf.options`. Este archivo de configuración principal generalmente se encuentra en el directorio `/etc/bind/` o `/etc/named/` en la mayoría de las distribuciones de Linux.

```
options {
allow-query-cache { none; };
recursion no;
};
```

Configuración DNS de Microsoft

En la herramienta de consola DNS de Microsoft:

a. Primero, haga clic derecho en el servidor DNS y haga clic en Propiedades.
b. Después de eso, haga clic en la pestaña Avanzado.
c. Finalmente, en las opciones del servidor, seleccione la casilla de verificación "Deshabilitar recursividad" y luego haga clic en Aceptar.

Configuración en postfix 3.x

En el archivo de configuración /etc/postfix/main.cf

En la variable “mydestination” NO deben estar los dominios locales:

```
localhost.localdomain, localhost
```

Aumentar los parametros (si no existiesen):

```
mynetworks_style = host
relay_domains =
```

Tambien es valido: mynetworks_style = subnet

Sugerencias a considerar

Utilizar cortafuegos compatibles con el DNS y utilizar protección DDoS de terceros.

Deshabilitar transferencia de zona

La vulnerabilidad de transferencia de zona en los servidores DNS es una vulnerabilidad de seguridad que permite a un atacante obtener copias completas de la zona de nombres de un servidor DNS. La zona de nombres de un servidor DNS es un archivo que contiene información sobre los nombres de dominio y sus correspondientes direcciones IP.

La transferencia de zona es un proceso legítimo utilizado por los servidores DNS para compartir información sobre los nombres de dominio entre ellos. Sin embargo, si la configuración del servidor DNS está mal configurada, un atacante puede aprovechar esta función legítima para obtener una copia completa de la zona de nombres, lo que le permitiría realizar ataques de denegación de servicio o identificar otros vectores de ataque.

Los servidores DNS mal configurados pueden permitir a cualquier persona solicitar una transferencia de zona sin autenticación o permitir la transferencia de zona a cualquier dirección IP. Si un atacante identifica que un servidor DNS es vulnerable a la transferencia de zona, puede utilizar herramientas disponibles públicamente para realizar la transferencia de zona y obtener información sobre los nombres de dominio y direcciones IP.

Es importante que los administradores de sistemas configuren correctamente los servidores DNS para evitar la vulnerabilidad de transferencia de zona y proteger la información confidencial. Las medidas de seguridad recomendadas incluyen restringir el acceso a la transferencia de zona solo a direcciones IP específicas y autenticar las solicitudes de transferencia de zona. Además, es importante mantener el software del servidor DNS actualizado con las últimas actualizaciones de seguridad para evitar vulnerabilidades conocidas.

Deshabilitar transferencia de zona (Bind)

En el archivo `/etc/bind/named.conf` adicionar:

```
options {
  allow-transfer {"none";};
};
```