Guía de estudio - Políticas de seguridad en la gestión de zonas DNS y asignación de IPs

¡Hola! Te damos la bienvenida a esta nueva guía de estudio.

¿En qué consiste esta guía?

El control de la seguridad en la gestión de zonas DNS y la asignación de direcciones IP es crucial para la estabilidad y protección de la infraestructura de red. Una configuración adecuada evita ataques como la suplantación de DNS, la inyección de registros falsos y la asignación indebida de direcciones IP.

En esta guía, exploraremos:

- Mejores prácticas para la seguridad en la gestión de zonas DNS.
- Políticas de seguridad para la asignación de direcciones IP.
- Configuraciones avanzadas para mitigar riesgos de seguridad.

¡Vamos con todo!

Tabla de contenidos

Guía de estudio - Políticas de seguridad en la gestión de zonas DNS y asignación de IPs 1
¿En qué consiste esta guía? 1
Tabla de contenidos 2
Seguridad en la gestión de zonas DNS 3
Configuración de seguridad en zonas DNS 3
Protección contra ataques de DNS 3
Actividad guiada: Configuración segura de zonas DNS 4
Políticas de seguridad en la asignación de direcciones IP 4
Configuración segura del servidor DHCP 4
Restricción de asignación de direcciones IP 4
Protección contra servidores DHCP ilegítimos (Rogue DHCP) 5
Actividad guiada: Configuración segura del servidor DHCP 5
Configuraciones avanzadas para seguridad DNS y DHCP 5
¡Manos a la obra! - Detección y mitigación de ataques a DNS y DHCP 6

¡Comencemos!

Seguridad en la gestión de zonas DNS

El Sistema de Nombres de Dominio (DNS) es esencial para la resolución de nombres en una red, pero también puede ser un vector de ataque si no se configura correctamente. Implementar políticas de seguridad sólidas es fundamental para evitar ataques como la suplantación de DNS y las consultas malintencionadas.

Configuración de seguridad en zonas DNS

- **Restringir transferencias de zona a servidores autorizados:**

```
Set-DnsServerZoneTransferPolicy -ZoneName "empresa.local" -AllowTransfer
OnlyToServers -NameServers "192.168.1.2"
```

- **Habilitar la validación de registros DNS para evitar registros fraudulentos:**

```
Set-DnsServerDsSettings -EnableDnsSec $true
```

- **Configurar registros protegidos en Active Directory (AD-integrated DNS):**

```
Set-DnsServerZoneAging -Name "empresa.local" -ScavengingState $true
```

Protección contra ataques de DNS

- **Deshabilitar la resolución recursiva si no es necesaria:**

```
Set-DnsServerSetting -DisableRecursion $true
```

- **Configurar listas de acceso para evitar consultas desde IPs no confiables:**

```
Set-DnsServerQueryResolutionPolicy -Name "RestrictExternal" -Action DENY
-ApplyOnRecursion -Fqdn "*.empresa.local"
```

- **Habilitar auditoría de eventos DNS para detectar actividades sospechosas:**

```
Set-DnsServerDiagnostics -All $true
```

Actividad guiada: Configuración segura de zonas DNS

1. Iniciar la máquina virtual con Windows Server Core 2019 sin Dominio.
2. Crear una zona primaria en el servidor DNS.
3. Configurar restricciones de transferencia de zona.
4. Habilitar DNSSEC para protección contra manipulaciones.

Políticas de seguridad en la asignación de direcciones IP

El Protocolo de Configuración Dinámica de Host (DHCP) es responsable de la asignación de direcciones IP en una red. Sin una política de seguridad adecuada, los atacantes pueden aprovecharse de direcciones IP no autorizadas para infiltrarse en la red.

Configuración segura del servidor DHCP

- **Autorizar el servidor DHCP en Active Directory:**

```
Add-DhcpServerInDC
```

- **Configurar la detección de conflictos para evitar duplicación de IPs:**

```
Set-DhcpServerSetting -ConflictDetectionAttempts 2
```

- **Habilitar auditoría de eventos DHCP:**

```
Set-DhcpServerAuditLog -Enable $true -Path
"C:\Windows\System32\dhcp\audit.log"
```

Restricción de asignación de direcciones IP

- **Configurar listas de control de acceso para direcciones IP específicas:**

```
Set-DhcpServerv4Filter -List Allow -MacAddress "00-1A-2B-3C-4D-5E"
```

- **Restringir la concesión de direcciones solo a clientes autenticados:**

```
2.3 Protección Contra Servidores DHCP Ilegítimos (Rogue DHCP)
Habilitar la detecc
```

Protección contra servidores DHCP ilegítimos (Rogue DHCP)

- **Habilitar la detección de servidores DHCP no autorizados:**

```
Get-DhcpServerInDC
```

- **Configurar la protección de red contra servidores DHCP no autorizados:**

```
Set-DhcpServerv4Filter -List Deny -MacAddress "00-FF-AA-BB-CC-DD"
```

Actividad guiada: Configuración segura del servidor DHCP

1. Iniciar la máquina virtual con Windows Server Core 2019 CON Dominio.
2. Instalar y autorizar el servidor DHCP en Active Directory.
3. Configurar filtrado de direcciones MAC.
4. Implementar auditoría de eventos DHCP.

Configuraciones avanzadas para seguridad DNS y DHCP

Medida de Seguridad	Descripción
DNSSEC (DNS Security Extensions)	Protege la integridad de las consultas DNS evitando falsificación de respuestas.
Registros protegidos en Active Directory	Asegura que solo dispositivos autorizados puedan registrar entradas en el DNS.
Filtrado de direcciones MAC en DHCP	Permite restringir qué dispositivos pueden obtener direcciones IP.
Auditoría de eventos en DNS y DHCP	Permite rastrear cambios y detectar actividad sospechosa.
Restringir el acceso a servicios DNS y DHCP	Configurar listas de control de acceso (ACL) para minimizar la exposición.

Tabla 01. Configuraciones avanzadas.
Fuente: ADL.

¡Manos a la obra! - Detección y mitigación de ataques a DNS y DHCP

1. Iniciar la máquina virtual con Windows desktop y la máquina virtual con Windows Server configurada en las actividades anteriores.
2. Simular una consulta DNS no autorizada desde la mv desktop a la mv Windows Server Core y verificar el bloqueo.
3. Revisar eventos de auditoría en el servidor DHCP.
4. Configurar restricciones de acceso para evitar ataques Rogue DHCP.

Reflexiona:

- ¿Cómo ayuda DNSSEC a mejorar la seguridad en la resolución de nombres de dominio?
- ¿Por qué es importante restringir la transferencia de zonas DNS?
- ¿Qué ventajas ofrece el filtrado de direcciones MAC en DHCP?
- ¿Cómo se pueden detectar servidores DHCP no autorizados en una red?
- ¿Cuáles son las mejores prácticas para auditar la seguridad en DNS y DHCP?

Las políticas de seguridad en la gestión de zonas DNS y asignación de IPs son esenciales para mantener una infraestructura de red segura. La implementación de medidas como restricción de transferencia de zonas, DNSSEC, auditoría de eventos y filtrado de direcciones MAC permite minimizar riesgos y evitar ataques.