Índice:

Ejercicio 1 2

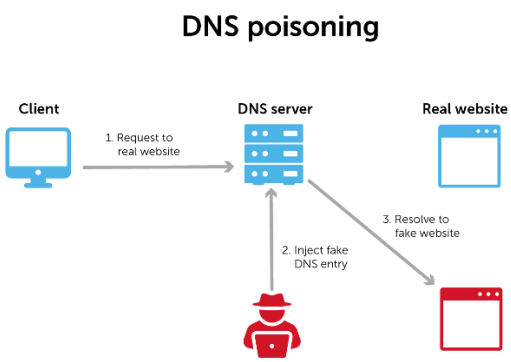
a) Elabora un informe de las vulnerabilidades del servicio DNS y las técnicas aplicadas para permitir seguridad en el servicio DNS. 2

Ejercicio 1

a) Elabora un informe de las vulnerabilidades del servicio DNS y las técnicas aplicadas para permitir seguridad en el servicio DNS.

A pesar de su importancia, el DNS es vulnerable a diversas amenazas que podrían comprometer la integridad, confidencialidad y disponibilidad de la información. Es muy importante conocer las vulnerabilidades y como mitigarlas con técnicas para proporcionar seguridad

1. **Cache Poisoning:**
   - *Descripción:* Este ataque explota la falta de autenticación en las respuestas DNS, permitiendo que un atacante introduzca datos falsos en la caché del servidor, provocando la resolución incorrecta de nombres de dominio.

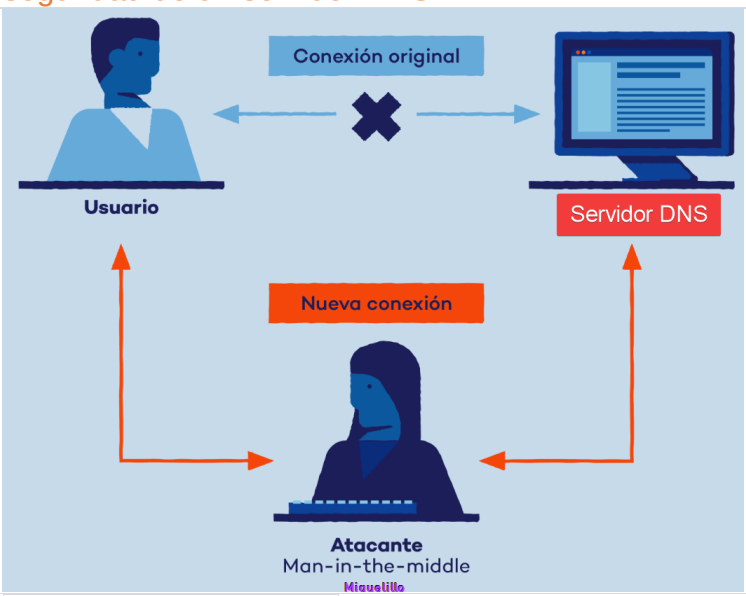


   - *Técnicas de Mitigación:* La adopción de DNSSEC se convierte en una defensa efectiva, ya que firma digitalmente los registros DNS, garantizando la autenticidad de los datos y evitando la manipulación de la caché.

2. **Ataques de Amplificación:**
   - *Descripción:* Ataques DDoS se intensifican mediante solicitudes falsificadas a servidores DNS abiertos, amplificando la magnitud del ataque y comprometiendo la disponibilidad de servicios.

   - *Técnicas de Mitigación:* Configurar servidores DNS para evitar ser utilizados como amplificadores y aplicar filtros de tráfico para bloquear patrones maliciosos, reduciendo la eficacia de ataques DDoS.

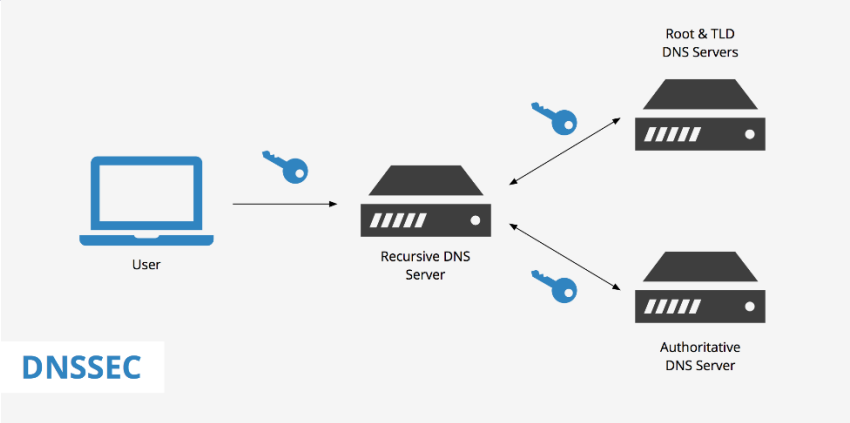
3. **DNS Spoofing:**
   - *Descripción:* conseguir modificar los registros que se almacenan en el servidor DNS por los que decida el atacante y para la cual se emplean diferentes mecanismos. Entre ellos, encontramos el DNS Cache Poisoning, pero también ataques Man-In-The-Middle, uso de estaciones base falsas o incluso comprometer la seguridad de un servidor DNS.



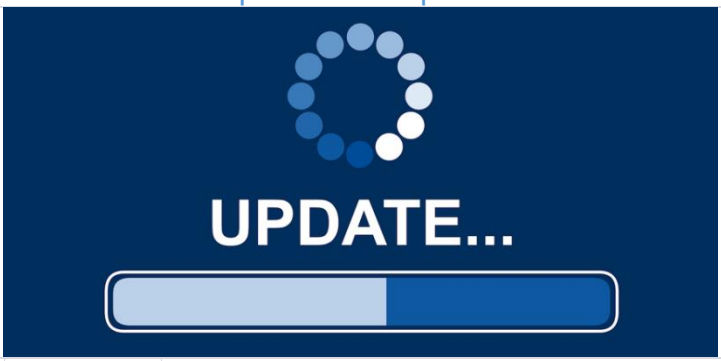
   - *Técnicas de Mitigación:* La implementación de sistemas de monitoreo puede detectar y prevenir este tipo de ataques, protegiendo la integridad y evitando redirecciones no autorizadas.

Técnicas para Mejorar la Seguridad del Servicio DNS:

1. **DNS Security Extensions (DNSSEC):**
   - *Descripción:* DNSSEC aborda la falta de autenticación en el DNS mediante la firma digital de registros DNS, garantizando la integridad de la información y previniendo manipulaciones maliciosas.



   - *Beneficios:* Al implementar DNSSEC, se establece una capa adicional de seguridad que protege contra vulnerabilidades como el cache poisoning, asegurando la confianza en la resolución de nombres de dominio.
2. **Actualizaciones y Parches Regulares:**
   - *Descripción:* Mantener el software DNS actualizado con parches de seguridad es esencial para prevenir la explotación de vulnerabilidades conocidas, garantizando la resistencia del servicio frente a posibles ataques.



   - *Beneficios:* Las actualizaciones regulares refuerzan las defensas del sistema, cerrando brechas de seguridad y mejorando la capacidad de respuesta a amenazas emergentes.

3. **Monitoreo Continuo:**
   - *Descripción:* La implementación de sistemas de monitoreo constante permite la detección temprana de actividades sospechosas o patrones anómalos, facilitando una respuesta rápida ante posibles ataques.

   - *Beneficios:* Al monitorear activamente el tráfico DNS y otros indicadores de compromiso, las organizaciones pueden identificar amenazas en tiempo real y tomar medidas proactivas para mitigar riesgos y proteger la estabilidad del servicio.