DNS Spoofing

Transcribed on August 2, 2025 at 11:27 AM by Minutes AI

Speaker 1 (00:01)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de los ataques IPV y en concreto de un ataque llamado DNS Spoofing.

El DNS spoofing es también conocido como envenenamiento de caché DNS.

Es un ataque en el que el atacante intercepta peticiones DNS y responde con direcciones IP falsas para redirigir a los usuarios a sitios maliciosos sin que estos se den cuenta.

El objetivo es engañar a los usuarios para que entreguen información sensible o descarga de un malware, por ejemplo.

En la diapositiva podéis ver un pequeño esquema que describe el flujo de ataque de un DNS spoofing.

Bien, pues ahora vamos a hacer una práctica asociada al DNS spoofing.

Como siempre aquí tengo dos máquinas y una va a actuar como atacante y la otra será la máquina que será atacada o también nuestro servidor.

Y para el ataque voy a usar una herramienta llamada DNS spoof o también ethercap que permite interceptar y alterar el tráfico DNS de una red.

Y bien, pues como herramienta utilizaré dnsspoof o ethercap que son herramientas que permiten interceptar y alterar el tráfico DNS de una red.

El paso principal será instalar la aplicación de DNS, para eso hay que utilizar un kit o un set de herramientas que se llama dsniff que lo podemos hacer como siempre.

Y ya hacemos el sudo apt install dsn if Le decimos que sí, ya lo tenemos.

Bien, pues el primer paso para poder utilizar dnsspuff es crear un fichero host.

En este fichero host ponemos un dominio y una dirección IP para que cada vez que se acceda a ese dominio se redireccione a la dirección IP.

Y en esa dirección IP montaremos un pequeño servidor web que será el que presentará una página que hemos diseñado nosotros con todo lo que queramos que se ejecute o que vea esa persona que piensa que va a la página principal.

Aquí ya podríamos simular por ejemplo el acceso de un usuario y una contraseña para obtener sus credenciales, etc.

Así que voy a crear el fichero con nano, le voy a llamar my new host, por ejemplo txt y aquí dentro pues haríamos 10 211 55 5 que es esta máquina y haremos que redireccione siempre a, por ejemplo, esta página web que la tenemos aquí.

Y aquí podemos ver la página web.

Vale, pues en vez de aparecer esta página pondremos nuestra propia página con nuestra información o con todas las técnicas que queramos utilizar para obtener algún tipo de información del usuario.

Bien, pues desde aquí ya almaceno y ahora voy a crear un pequeño servidor web muy sencillo con el código mínimo HTML que sea la página que suplanta a la principal de ciberalles.

Entonces lo que haremos será hacer un nano index HTML que es la página principal, que ya sabéis que es así cuando es una página web.

Entonces con nano HTML pues aquí crea, damos una web.

Bien, pues se ha creado este pequeñísimo y simple código en HTML que lo que va a hacer es mostrar ese texto que veis ahí simplemente a cambio de lo que tendría que verse de la página principal.

Entonces ya con esto al menos nos puede servir para que tengáis un poco visión del concepto y de la base del ataque.

Bien, pues ahora como ya hemos hecho en otros ejercicios voy a levantar un pequeño servidor en Python para que se pueda ver esa página index HTML que la tengo aquí por algún sitio.

Aquí está.

Entonces haríamos un python y levantaríamos con guión m y pondríamos HTTP server puerto 8000 por ejemplo y lo lanzamos.

En este momento estamos ya publicando nuestra página.

Si yo ahora me voy aquí al localhost 8000 vamos a verlo ahí.

Está es la página que en teoría va a suplantar a la original.

Aquí podríamos poner de todo, podemos hacerla muy parecida a la otra con pequeños cambios también con formularios para que metan usuario y contraseña, información personal, lo que sea.

La cosa es que el usuario piense que está entrando en la web que pensaba entrar, que era la que tenía por defecto en mente acceder, pero realmente le hemos redirigido a otra totalmente diferente para hacer cualquier tipo de captura de información que queramos hacer en ese momento.

Vale, pues dejamos aquí este, Voy a abrir otro terminal para no parar en el servidor web y ahora sí por fin vamos a levantar dnsspuf.

Para ello haremos este comando que como ya podéis imaginar lo que hace es que prepara la interfaz eth, en mi caso f, simplemente nos dice la ruta del host, entonces le pondremos aquí el nombre del host, sería my new host y poco más, porque ya en el momento que lanzamos esto dnss ya empezará a escuchar la red buscando peticiones y solicitudes DNS cuando reciba una petición para uno de los dominios que hemos especificado en el fichero hostia dnspuff lo que va a hacer es responder con la IP falsa y lo va a dirigir al usuario al sitio que está controlado por el atacante.

Así que vamos a ir un momento a la máquina que va a ser atacada, que está en la misma DEP que justamente esta que tiene la dirección IP.

Bien, pues ya hemos confirmado que tenemos levantado la página web para redireccionar de Ciberaves y también hemos visto que tenemos la aplicación DNS funcionando.

Entonces ahora desde esta máquina, si hacemos un ping a cyberaves, veremos que ya está redireccionando, fijaros, ya no está direccionando hacia la dirección IP pública que tiene.

Con lo cual en este punto vemos que ha tenido éxito.

El DNS está desviando todo el tráfico que va hacia la página de ciberades, pero la está direccionando hacia la web que tenemos en la 10.211.55.17.

También se puede comprobar si abrimos el navegador bien, y como podéis ver, lo que está redireccionando es hacia el pequeño servidor web que hemos montado antes.

Con lo cual, 100 % de éxito.

En este momento todo el tráfico DNS lo estamos capturando nosotros y lo estamos desviando hacia donde queremos.

Claro, aquí es muy obvio que esta no es la página orig.

Que ya visteis de Ciberdex, pero imaginaros que la suplantamos con una página muy parecida, una página similar, y hacemos que el usuario crea que está en su página web, por ejemplo, de trabajo o de lo que sea.

Con lo cual estaríamos ahí consiguiendo información de todo tipo, poniendo por ejemplo falsas entradas de contraseña o de información.

Volviendo al servidor, para que veáis que todo está funcionando bien, aquí estamos viendo las peticiones tanto internas como remotas que yo tengo por aquí, y también aquí tengo lanzado pues el Tenace Spoof, aquí lo veis que está.

Está funcionando.

Y también podemos ver aquí que localmente también estaba funcionando la página web, que ya sabéis que la página web original en principio era esta que podéis ver aquí.

Bien, pues en este punto ya hemos visto que el ataque ha funcionado.

Por supuesto que tiene algunas consideraciones.

Por ejemplo, es conveniente que la máquina, bueno, de hecho tenemos que hacer lo que la máquina que hace de cliente tenga puesta como DNS la IP del servidor.

Esto es normal, porque tú cuando tienes un entorno empresarial o un entorno más o menos serio, las direcciones IP que tú asignas son estáticas, por lo menos también para las DNS.

Tú tienes tu propio servidor DNS, eso habrá que ponerlo manualmente en la máquina cliente para que siempre apunte al DNS tuyo, aunque en este punto lo estamos suplantando.

Nosotros estamos tomando el control desde el fichero conf que visteis antes que poníamos la dirección IP y asociada a un dominio, y ahí ya empezaríamos a configurar nuestro ataque con el DNSSPUFF.

Si nos centramos en la mitigación, tenemos por ejemplo DNSSEC, que son extensiones de seguridad del sistema de nombres de dominio y esto le añade una capa de autenticación a las respuestas DNS.

Esto dificulta muchísimo que los atacantes manipulen las respuestas DNS sin que sean detectadas.

Por este motivo tenemos que usar servidores DNS con validación DNSSEC, porque de esta forma se puede verificar la firma digital de las respuestas DNS y prevenir respuestas falsificadas.

También tenemos que configurar cortafuegos y filtros IDS IPS para detectar y bloquear tráfico DNS sospechoso o malicioso.

Estas herramientas pueden identificar patrones de tráfico anormales o conocidos asociados con ataques de DNS spoofing.

También hay que mantener siempre actualizado el software del servidor DNS, porque si lo actualizamos de forma regular estaremos aplicando una protección estaremos preparados para cualquier técnica nueva que aparezca de ataque.

Habría muchas más, como por ejemplo realizar análisis de tráfico DNS continuo o aplicar políticas de seguridad muy estrictas en el manejo de las DNS internamente, etc.

Pero estas son al menos algunas de las principales.

Las estrategias de mitigación contra ataques DNS spoofing son fundamentales para proteger nuestra arquitectura.

Implementar DNSSEC proporciona una capa robusta de autenticidad y seguridad en las respuestas DNS, lo que dificulta mucho los ataques.

Además, el uso de servidores DNS que validen las firmas digitales es crucial para asegurar también nuestra arquitectura.

Por otro lado, configurar de forma adecuada cortafuegos y sistemas de detección y prevención de intrusiones como los IDS y los ips tienen un papel fundamental en la identificación y bloqueo de tráfico DNS malicioso, protegiendo así contra ataques de spoofing.

Llegamos al final de la sesión, os esperamos en el siguiente vídeo.