Spoofing

1.- Objetivo

* El objetivo de este trabajo es explicar y mostrar uno de los ataques más recientes descubiertos en Internet, la técnica *Web Spoofing*.
* Para ello, se ha procedido a la implementación de esta técnica demostrando la vulnerabilidad de los dos navegadores más populares: *Microsoft Internet Explorer* y *Netscape Navegator*.

2.- Resumen

En este trabajo se estudia la técnica *Web Spoofing* como método de ataque a través de Internet. Se trata de una variante del clásico ataque *man-in-the-middle* en el que un ordenador intermedio analiza y registra información sensible. Además, se analizan los diferentes aspectos a considerar a la hora de aplicar esta técnica así como los detalles de la implementación realizada para mostrar su funcionamiento. Por último, se presentan una serie de contramedidas que el usuario puede adoptar con objeto de protegerse de este tipo de ataques.

3.- Marco Teórico

**Spoofing**, en términos de [seguridad](https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica) de [redes](https://es.wikipedia.org/wiki/Red_de_computadoras) hace referencia al uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.

El término *spoof* significa engaño, truco, trampa o burla. Existen diversas técnicas informáticas de *Spoofing* basadas en falsear direcciones de correo electrónico (*MailSpoofing*), direcciones IP (IP *Spoofing*), direcciones MAC (MAC *Spoofing*), servidores de nombres de dominio (DNS *Spoofing*), etc. La técnica *Web Spoofing* se realiza en el entorno *World Wide Web* y su principal objetivo es falsear un sitio web de confianza para la víctima (por ejemplo, el sitio web de su empresa, su banco, etc.) La técnica en sí es una variante del clásico ataque *man-in-the-middle*  en el que un ordenador intermedio analiza y registra información sensible (ataque pasivo) o incluso la modifica en ambos sentidos (ataque activo).

### ¿Cómo funciona el ataque de Spoofing?

El spoofing entran en juego tres máquinas: **un atacante**, **un atacado**, y **un sistema suplantado** que tiene cierta relación con el atacado; para que el pirata pueda conseguir su objetivo necesita por un lado establecer una comunicación falseada con su objetivo y por otro evitar que el equipo suplantado interfiera en el ataque.



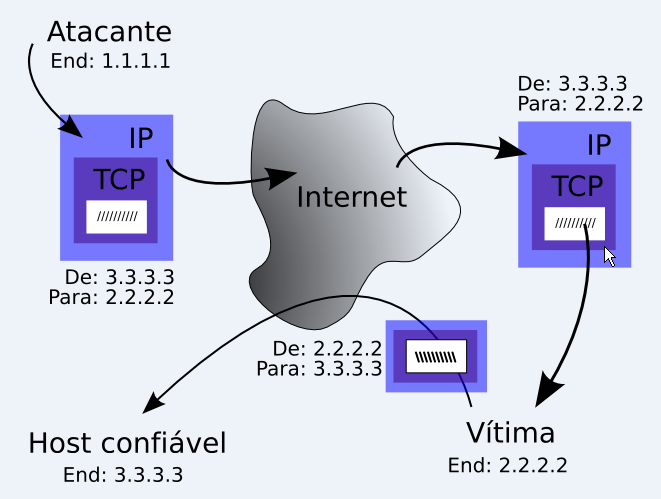
Podemos comprobar que el spoofing no es inmediato; de entrada, el atacante ha de hacerse una idea de cómo son generados e incrementados los números de secuencia TCP, y una vez que lo sepa ha de conseguir engañar a su objetivo utilizando estos números para establecer la comunicación; cuanto más robusta sea esta generación por parte del objetivo, más difícil lo tendrá el pirata para realizar el ataque con éxito.

Es necesario recordar que el spoofing es un ataque ciego: el atacante no ve en ningún momento las respuestas que emite su objetivo, ya que estas van dirigidas a la máquina que previamente ha sido deshabilitada, por lo que debe presuponer qué está sucediendo en cada momento y responder de forma adecuada en base a esas suposiciones.

Sería imposible tratar con el detenimiento que merecen todos los detalles relativos al spoofing por lo que para obtener información adicional es necesario dirigirse a excelentes artículos que estudian todos los pormenores del ataque, como o de la misma forma, para conocer con detalle el funcionamiento del protocolo TCP/IP y sus problemas podemos consultar.

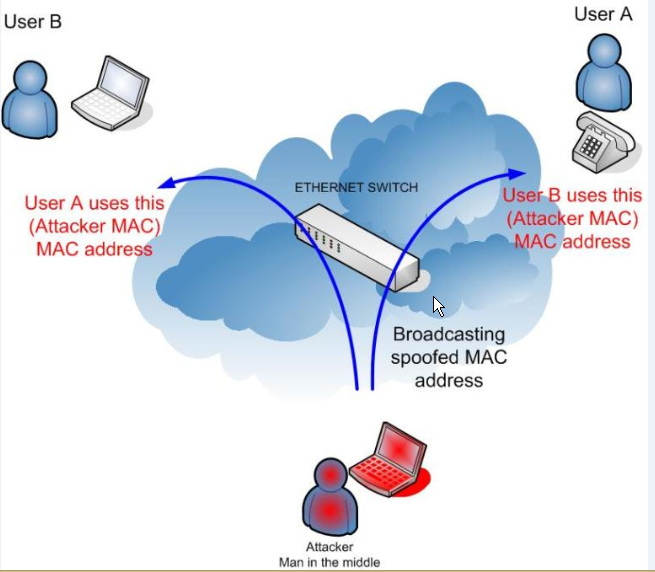
Se pueden clasificar los ataques de *spoofing*, en función de la [tecnología](https://es.wikipedia.org/wiki/Tecnolog%C3%ADa) utilizada. Entre ellos tenemos el [IP](https://es.wikipedia.org/wiki/Protocolo_IP) spoofing (quizás el más conocido), ARP spoofing, DNS spoofing, Web spoofing o email spoofing, aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

**IP Spoofing**

* Consiste básicamente en sustituir la dirección IP de origen en un paquete TCP/IP por otra dirección IP a la cual se desea suplantar.
* Puede ser usado para cualquier protocolo dentro de TCP/IP.
* Hay que tener en cuenta que las respuestas del host que reciba los paquetea alterados irán dirigidas a la IP falsificada.
* 

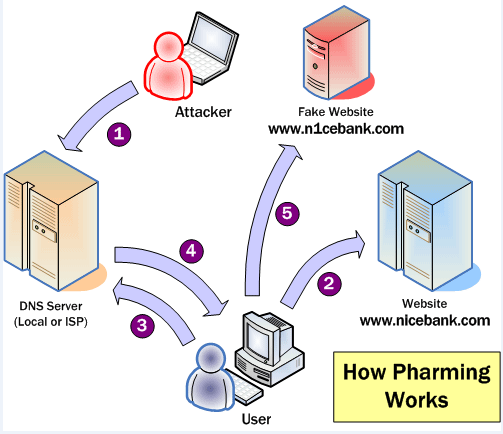
**ARP Spoofing**

* El protocolo Ethernet trabaja mediante direcciones MAC que es la construcción de tramas de solicitudes y respuestas ARP modificadas con el objetivo de falsear la tabla ARP (relación IP-MAC) de una víctima.
* Forza paquetes a un host atacante en lugar de hacerlo a su destino legitimo.
* Dicha tabla ARP puede ser falseada por un ordenador atacante que emite tramas ARP\_REPLY indicando su MAC como destino valido para un IP.



**DNS Spoofing**

* Se trata del falseamiento de una relación “Nombre de dominio-IP” ante una consulta de resolución de nombre, es decir, resolver con una dirección IP falsa un cierto nombre DNS O viceversa.



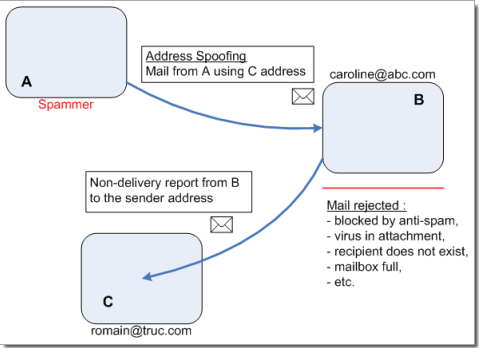
**WEB Spoofing**

* En ruta conexión de una víctima a través de una página falsa hacia otras páginas WEB con el objeto de obtener información de dicha victima (páginas web vistas , información de formularios, contraseñas).



**E-MAIL Spoofing**

* El llamado mail Spoofing es la técnica mas frecuente de propagación de virus de este tipo, el cual funciona suplantando el correo electrónico de la dirección de e-mail de nuestros contactos.



4.- Conclusión

* Es una metodología o técnicas de suplantación de identidad de algún usuario con uso malicioso par obtener información confidencial usando protocolos como ARP, IP, DNS, HTTP.
* Definir listas de control de acceso en el router frontera.
* Contar con switch administrable que permita el manejo de la tabla de direcciones MAC, el estado y negociación de los puertos.
* Utilizar la autenticación de claves entre la comunicación de la red utilizando IPSEC.
* Existen herramientas que permiten detectar si somos víctimas de SPOOFING, por ejemplo analizador de tráfico (wireshark).

4.-Bibliografia

* [1] R. Graham, *Hacking Lexicon*, on-line: http://www.robertgraham.com/pubs/hacking-dict.html, march 8, 2004.
* [2] T. Berners-Lee, R. Fielding, U.C. Irvine, and L. Masinter, *Uniform Resource Identifiers (URI): Generic*
* *Syntax*, on-line: http://www.ietf.org/rfc/rfc2396.txt, The Internet Engineering Task Force (IETF), january, 1999.
* [3] E.W. Felten, D. Balfanz, D. Dean, and D.S. Wallach, *Web Spoofing: An Internet Con Game*, on-line:
* http://www.cs.princeton.edu/sip/pub/spoofing.html, 1996.