Seguridad en redes: Spoofing y phishing

Fundamentos de redes
Universidad de Granada

Gallardo Morales, Juan Carlos
Izquierdo Vera, Javier

13 de diciembre de 2015

Índice

Índice de figuras

1. Introducción

Decir que internet está empezando a formar parte de nuestra vida cotidiana ya es quedarse atrás, internet está presente en nuestro día a día y cada vez es utilizado por más gente y para más funciones. Es por ello que la seguridad se ha vuelto un factor muy importante en la red.

Vamos a hablar de dos tipos de ataques frecuentes que pueden comprometer nuestra privacidad y la integridad de nuestros sistemas, y estos son *spoofing* y *phishing*. Ambos son dos formas de ataque en la que el atacante busca engañarnos (a nosotros o a nuestra máquina) para así obtener datos privados o lograr comprometer nuestra máquina. Mediante un ataque de spoofing o phishing, el atacante podría obtener las credenciales de nuestra cuenta bancaria, o de nuestra red social favorita, o incluso del servidor de nuestra empresa.

El objetivo de este texto es explicar en qué consisten estas formas de ataque y cómo se realizan, para así poder prevenirlas y mejorar nuestra seguridad.

2. Spoofing

El spoofing, del inglés “spoof“, traducido al español como “parodia”,“burla”, “broma” [24], se basa en un conjunto de técnicas por la cual una persona (atacante) se hace pasar por otra entidad distinta para recolectar información confidencial de una entidad concreta (víctima) [7]; o dicho de otro modo, se basa en suplantar la identidad de un usuario o servidor, generalmente con intenciones maliciosas [22]. Esta técnica básicamente se nutre de las aplicaciones que utilizan el protocolo TCP/IP y no proporcionan mecanismos de verificación sobre la identidad del host de envío o recepción [5].

3. Tipos spoofing

Como veremos a continuación más detalladamente, existen muchos tipos de spoofing, entre los que destacamos ARP Spoofing, DNS Spoofing, IP Spoofing, E-mail Spoofing, Web Spoofing y GPS Spoofing.

3.1. ARP Spoofing

ARP es un protocolo de comunicación de la capa enlace que se basa en traducir direcciones IP a direcciones MAC. Recordemos que la dirección MAC es única para cada tarjeta de red, y que para que esa traducción sea posible se envía un paquete a *broadcast* con la IP solicitada para que la máquina con dicha IP le responda con su propia dirección MAC. Sin embargo, para ahorrar tiempos, cada enrutador y host mantiene una tabla ARP en caché con las traducciones anteriormentes dichas. [6]. El **ARP Spoofing** (comúnmente llamado “envenenamiento de tablas ARP”) se basa en modificar las tablas ARP de tal forma que para una determinada IP se haga válida la dirección MAC del atacante. De esta forma la información que va dirigida hacia dicha IP podrá pasar por el atacante que hará lo que vea conveniente con ella. [7, 25]

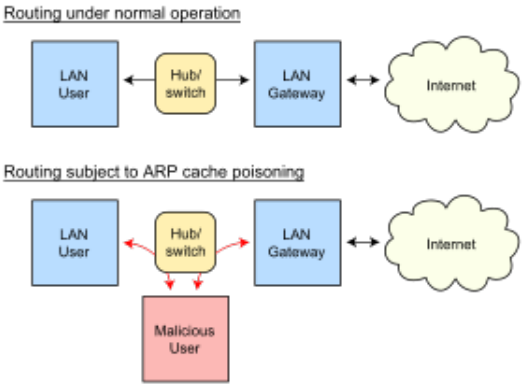

Figura 1: Esquema ARP Spoofing [12]

3.2. DNS Spoofing

En resumidas palabras el **DNS** es un sistema de traducción de nombres de dominio a direcciones IP, es decir, es un sistema que traduce las direcciones IP de los diferentes equipos de la red a nombres comunes más sencillos de recordar [22]. Sabiendo esto ya podemos decir que el **DNS Spoofing** se basa en el falseamiento de una dirección IP ante una consulta de resolución de nombres, es decir, resolver con una dirección IP distinta a la correspondiente para un cierto nombre DNS, o viceversa, sobre la máquina objetivo [25]. Cuando un usuario pide al servidor DNS que le resuelva un determinado nombre de dominio, este servidor le devuelve la IP perteneciente a dicho dominio. En el caso del DNS Spoofing se modifica dicho servidor DNS para que devuelva una dirección IP falsa al cliente que pidió la IP del dominio solicitado. [23] Para verlo más claro podemos consultar estas dos imágenes tomadas de [23]:

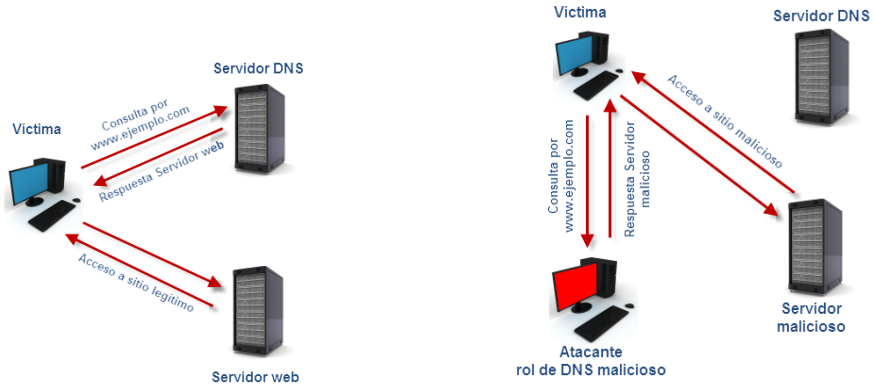

Figura 2: Esquema de DNS Spoofing [23]

3.3. IP Spoofing

La **IP Spoofing** es el tipo de spoofing más conocido en la actualidad. Su idea básicamente es enviar un paquete TCP/IP con la IP origen modificada para que el destinatario crea que viene de otra localización de confianza[17], es decir, permite suplantar a otra IP que la víctima detecta como fiable. Esto puede ocasionar que las respuestas del host puedan ir dirigidas a una IP falsa. Este tipo de ataque puede conseguirse con multitud de programas especializados en ello y sirve tanto para TCP, UDP y ICMP. [2]

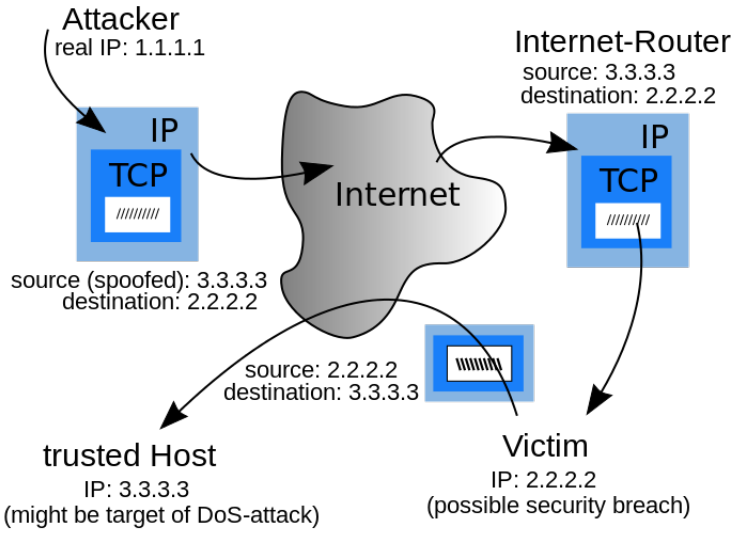

Figura 3: Esquema IP Spoofing [4]

3.4. E-mail Spoofing

En pocas palabras es el tipo de spoofing relacionado con la falsificación de los correos electrónicos. Para ello el atacante modifica la cabecera de un correo para que la víctima crea que éste ha sido enviado desde otro remitente. Esto lo podemos hacer modificando los campos “from”,“Return-Path” and “Reply-To”. Este tipo de ataque es posible ya que el protocolo SMTP (protocolo principal para enviar correos electrónicos) prescinde de autenticación. Normalmente este tipo de ataque es usado para el *SPAM* y el *PHISHING*, el cual veremos en qué consiste y algún ejemplo práctico posteriormente.

3.5. Web Spoofing

Se basa en enrutar o redirigir las solicitudes de un usuario hacia un servidor intermedio (web falseada) el cual actúa como proxy entre el cliente y la web original. De esta forma es posible recibir y modificar todos los datos del usuario para mandarlos al servidor original sin que el usuario se de cuenta de nada. Para ello tan solo tendríamos que modificar el archivo “hosts” por medio de cualquier malware, por ejemplo un troyano. Este archivo es utilizado para configurar redes locales y tan solo tendríamos que poner el nombre del host y la IP de la página web falsa, mientras que el phishing clona este servicio. [14]

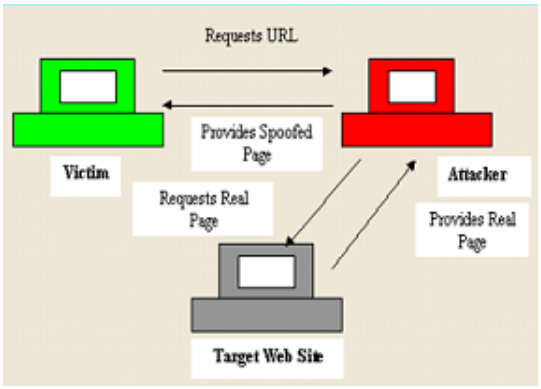

Figura 4: Esquema Web Spoofing [21], máquina atacante actuando como proxy

3.6. GPS Spoofing

Consiste en emitir una señal falsa creada a partir de la original, de modo que se emita a una frecuencia superior a la original para que la máquina objetivo finalmente acabe aceptando esta señal, reemplazando la original. [18, 19]

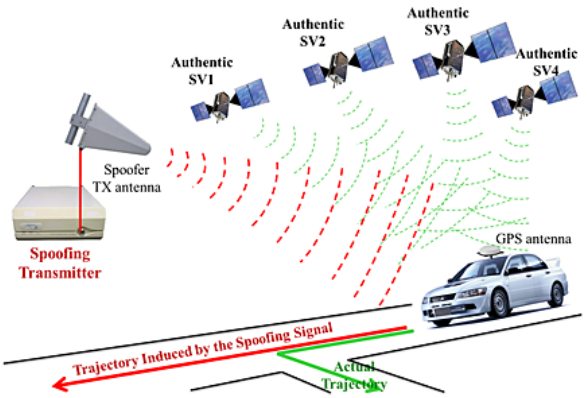

Figura 5: Esquema de GPS Spoofing a un navegador de un coche [3]

4. Phishing

El phishing es un método que consiste en la copia casi idéntica de un servicio o web, con el objetivo de confundir a usuarios. De este modo el atacante busca obtener cierta información confidencial del usuario, o que acceda o adquiera algo que proporcione cierto interés al atacante. Un ejemplo típico sería una dirección DNS muy parecida a la de un servicio que la víctima suele utilizar, para que de este modo, ya sea por medio de la ingeniería social (confundir al usuario para que utilice el enlace proporcionado por el atacante), o incluso por una errata escribiendo la dirección, la víctima acabe en un web que aparentemente es la que deseaba, y en ella introduzca, por ejemplo, sus credenciales.[13, 11, 16]

5. Diferencia entre spoofing y phishing

Una vez conocidas las definiciones de spoofing y phishing, pueden apreciarse las diferencias aunque estén relacionados. En el spoofing el objetivo es suplantar a una entidad confundiendo a la máquina de la víctima, es decir, modificando paquetes, tablas ARP, etc. Sin embargo, en el phishing no se suplanta la identidad de una entidad, no se confunde a la máquina, se confunde al usuario. El phishing se basa en realizar una copia del servicio original y engañar al usuario para que lo utilice. Un error típido es confundir web spoofing y phishing, la diferencia entre ambos es que web spoofing no clona la web, no busca simularla, sino que busca suplantarla de modo que el atacante actúe de proxy en la conexión, la víctima se conecta al atacante y el atacante realiza la conexión, pudiendo así interferir a su gusto. [14]

6. Prevención

Prevenir el spoofing y el phishing no es algo trivial. Como hemos visto anteriormente hay muchos tipos de spoofing y cada uno se basa en vulnerabilidades diferentes. Por ello lo más correcto sería explicar cómo podemos prevenir cada uno de los tipos vistos en las secciones anteriores.

- **ARP spoofing**: esta técnica solo puede llevarse a cabo en redes LAN y una manera de evitarlo sería teniendo tablas ARP estáticas (con IPs fijas), teniendo software de detección de cambios ARP y evitar cambios en las direcciones MAC mediante la seguridad de puerto

de los switches. Aún así es muy complicado detectarlo y una manera básica sería comprobar la tabla ARP (arp -v en el caso de Linux) detectando varias IPs con la misma dirección MAC asociada. [1]

- **DNS spoofing**: uno de los errores más comunes que se da en la mayoría de los hogares es dejar el acceso al router (192.168.1.1) con el usuario y contraseña por defecto, con lo que cualquiera que entre en nuestra red podrá modificar los parámetros relacionados con el DNS. Por lo tanto, la máxima recomendación para evitar el DNS spoofing es cambiar la contraseña de acceso a nuestro router.
- **IP Spoofing**: es una técnica muy complicada de realizar actualmente por los altos mecanismos de seguridad que nos brindan nuestros proveedores. Aún así se utiliza para otros ataques populares como Denegación de Servicio (DOS) por lo que es importante estar protegido. Para ello podemos modificar la lista de acceso de entrada de nuestro router (ACL) para bloquear direcciones privadas por debajo de nuestra interfaz de red y bloquear la salida de paquetes cuya IP origen no pertenezca a la subred; de esta forma evitaremos que se mande tráfico “spoofeado”. Otra recomendación es utilizar Ipv6 que trae incluidos mecanismos de cifrado y autentificación. [2]
- **Email spoofing**: este tipo de ataques se puede evitar usando firmas digitales en el correo electrónico para asegurar que los emails son de quienes dicen ser y evitando introducir datos confidenciales.
- **Web spoofing**: se trata de un ataque muy peligroso ya que es muy difícil de detectar. Algunas recomendaciones para prevenirlo son utilizar algún plugin del navegador para ver la IP del servidor en todo momento y no acceder a una web desde algún hipervínculo procedente de un email. Otra recomendación más drástica sería desconectar Javascript del navegador [8].
- **GPS spoofing**: aún no hay sistemas de prevención eficaces ya que por ejemplo, encriptar la señal emitida por los satélites aumentaría los costes exponencialmente, aumentar la frecuencia de las ondas GPS también requeriría una fuerte inversión económica. El método de prevención más defendido es utilizar algoritmos anti-spoofing capaces de medir la intensidad de señal y potencia y alertar al receptor si se detecta alguna anomalía. [15]

  La mayoría de los ataques **phishing** provienen de correos electrónicos que buscan engañarnos como usuarios. Son mensajes que intentan llamar la atención de quien los lee para que esta persona acceda a una web falsa o simplemente se descargue algún fichero con algún tipo de malware. La máxima recomendación, es no acceder a ningún hipervínculo proveniente de cualquier correo electrónico. [10]

7. Ejemplo de DNS spoofing y phishing con swad

Para realizar este ejemplo se utilizará como máquina atacante un sistema con Kali Linux 2.0 (192.168.43.2) y una máquina víctima con Windows 10 (192.168.43.3). Ambas se encuentran conectadas en lan mediante un router móvil.

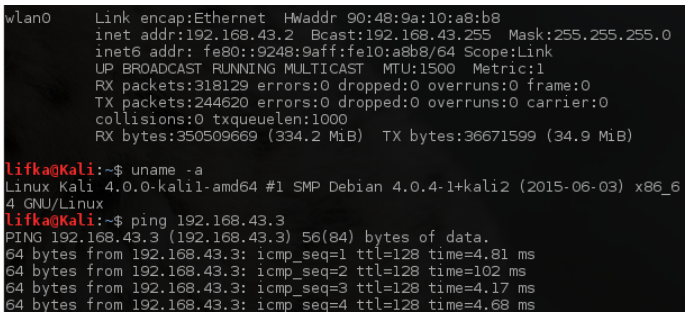

Figura 6: Máquina atacante (Kali) conectada a la misma red que la máquina víctima (Windows 10)

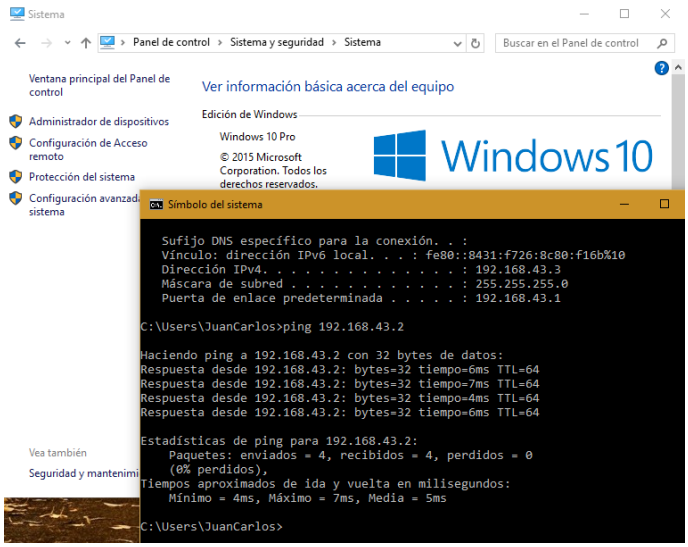

Figura 7: Máquina víctima (Windows 10) conectada a la misma red que máquina atacante (Kali)

El objetivo será realizar un phishing de la plataforma swad y lograr que la víctima lo utilice. Para ello engañaremos a la víctima utilizando Spoofing DNS mediante un ataque Man in the Middle utilizando ARP Spoofing, de modo que se modificará la traducción del DNS de swad a la IP del atacante para así lograr que la víctima no sospeche y el atacante pueda obtener sus credenciales si la víctima trata de autenticarse.

El primer paso será realizar el phishing de swad. Para ello se utilizará una herramienta llamada The Social-Engineer Toolkit (SET) desde el PC atacante. SET permite realizar distintos ataques relacionados con la ingeniería social, entre ellos realizar phising [20].

Figura 8: Iniciamos SET desde la máquina atacante

Utilizaremos el menú que nos ofrece para seleccionar la opción que nosotros deseamos. Primero elegimos “Social-Engineering Attacks” (opción 1), a continuación “Website Attack Vectors” (opción 2), ya que se trata de un ataque web. Y ahora seleccionamos la categoría de ataque de credenciales “Credential Harvester Attack Method” (opción 3). Ahora nos muestra solo 3 opciones:

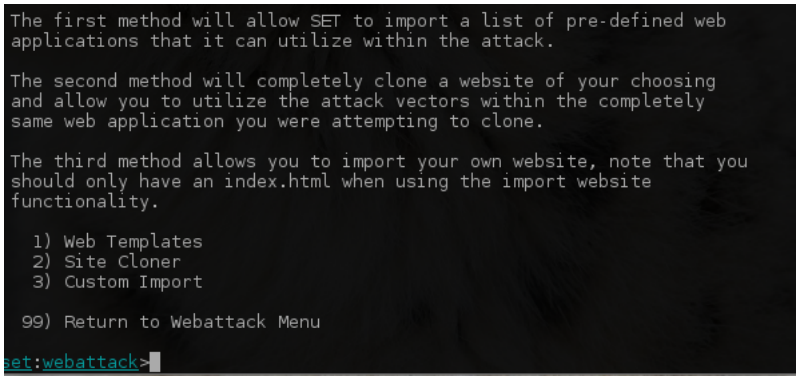

Figura 9: Disponemos de tres opciones diferentes para realizar un ataque de credenciales vía web utilizando SET

Seleccionaremos la opción 2, “Site Cloner”, que clonará completamente la web de swad.

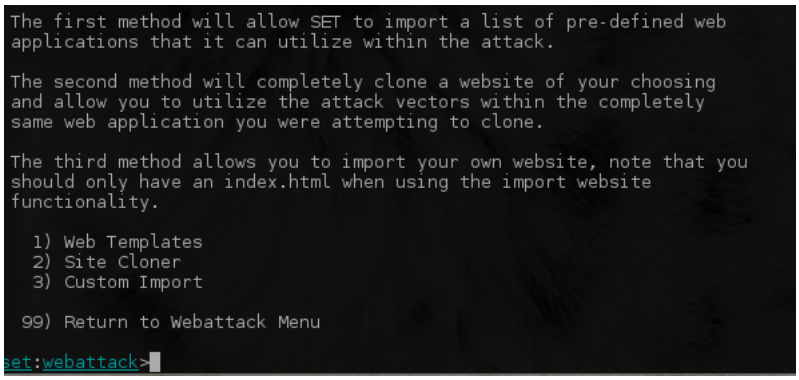

Figura 10: Iniciamos SET desde la máquina atacante

Nos pide establecer dos variables. En primer lugar nos pregunta la IP en la que se realizará el clon de la web, indicamos la IP del atacante (es la IP que se usará en las direcciones de la web clon). Tras eso, nos pide la url de la web que se desea clonar, indicamos la de swad (`http://swad.ugr.es`). Al terminar veremos como un clon de swad se ha guardado en */var/www/html*, podemos visitarlo usando el navegador:

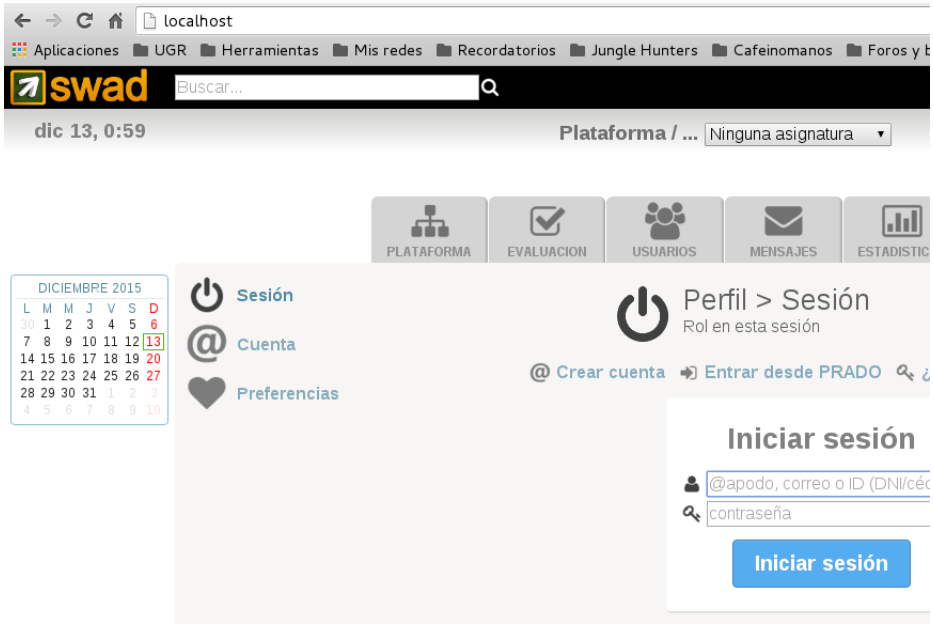

Figura 11: swad clonado utilizando SET

Una vez comprobado que tenemos la copia de la web en nuestro servidor, ya podemos realizar el ataque a la máquina víctima con el objetivo de conseguir que se conecte a la IP del atacante en lugar de la IP del dominio original y así utilice el clon de swad.
El siguiente paso será usar [9] para hacer DNS Spoofing. Ettercap es un sniffer con capacidad de interceptar y modificar paquetes. Vamos a utilizarlo para hacer que todas las conexiones de la máquina víctima sean interceptadas por ettercap. [9] En primer lugar configuraremos el archivo */etc/ettercap/etter.dns* para indicar que redirija las conexiones a swad hacia la máquina atacante, para ello:

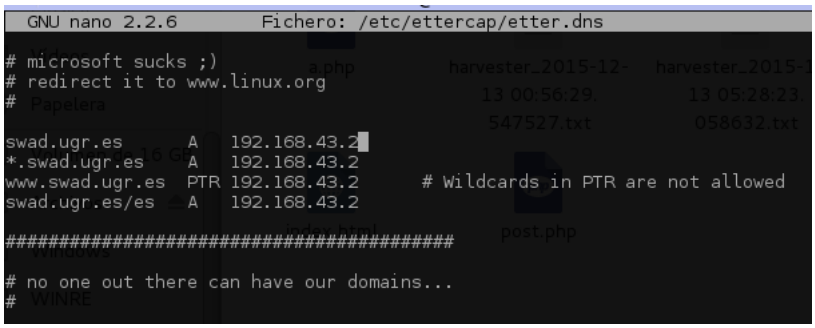

Figura 12: Configurando ettercap para redirigir las conexiones DNS a una IP diferente

A continuación comenzaremos a escuchar todas las conexiones que se producen en la red. Abrimos ettercap en su versión gráfica y vamos a la pestaña “Sniff”, seleccionando posteriormente “Unified Sniffing” y marcando nuestra tarjeta de red:

```
sudo ettercap -G
```

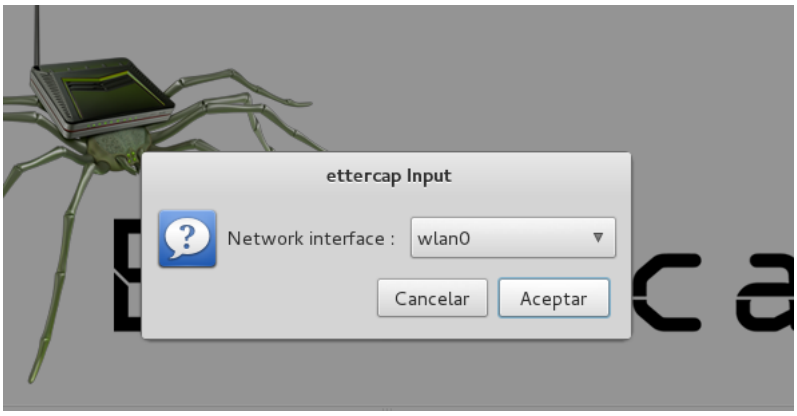

Figura 13: Vamos a sniffar la red con ettercap

Ahora buscaremos los dispositivos que se hayan conectados en nuestra red. Para ello desde la pestaña “Hots” seleccionamos la opción “Scan for hots”. Ettercap comenzará a escanear la red y mostrará los dispositivos disponibles:

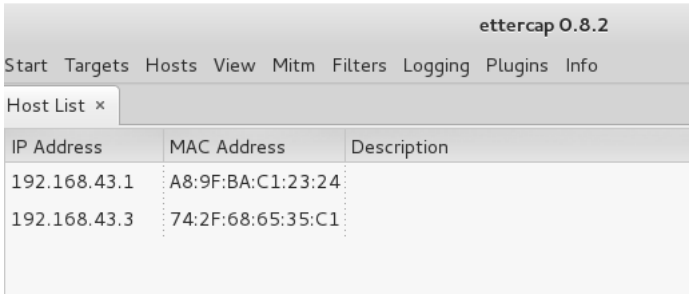

Figura 14: Hosts encontrados en la red con ettercap

Ettercap ha encontrado dos hosts, el router y la víctima. En este caso ya sabíamos la IP de la víctima, pero en caso de no conocerla de este modo podríamos haberla averiguado. A continuación vamos a guardar la dirección del router y la de la víctima en ettercap, para ello seleccionamos el router y lo marcamos como el primer objetivo (“Target 1”), y la víctima como el segundo objetivo (“Target 2”). Gracias a esto podremos hacer el DNS Spoofing por medio de los plugins que nos ofrece ettercap. Nos dirigimos a la pestaña “Plugins” y seleccionamos “Manage

the plugins", esto provocará que se nos abra una nueva pestaña mostrando todos los plugins disponibles. Seleccionamos "dns_spoof" haciendo doble click.

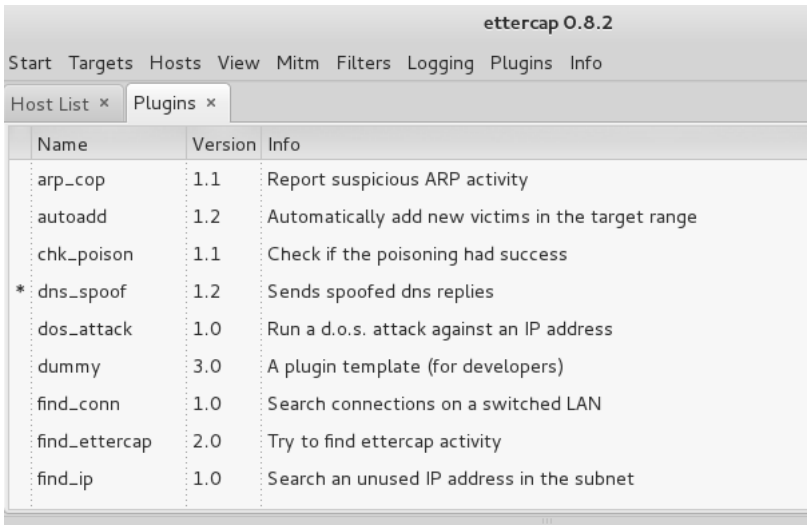

Figura 15: Seleccionado plugin para realizar DNS Spoofing en ettercap

Para realizar este DNS Spoofing tendremos que intervenir en la conexión de la víctima, para ello es necesario realizar un ataque Man in the Middle haciendo un ARP Spoofing. Una vez más, ettercap nos facilita todo el trabajo, nos dirijimos a la pestaña "MITM" (Man In The Middle) y seleccionamos "ARP Poisoning" (ARP Spoofing), marcando la opción que nos permite sniffar todas las conexiones remotas.

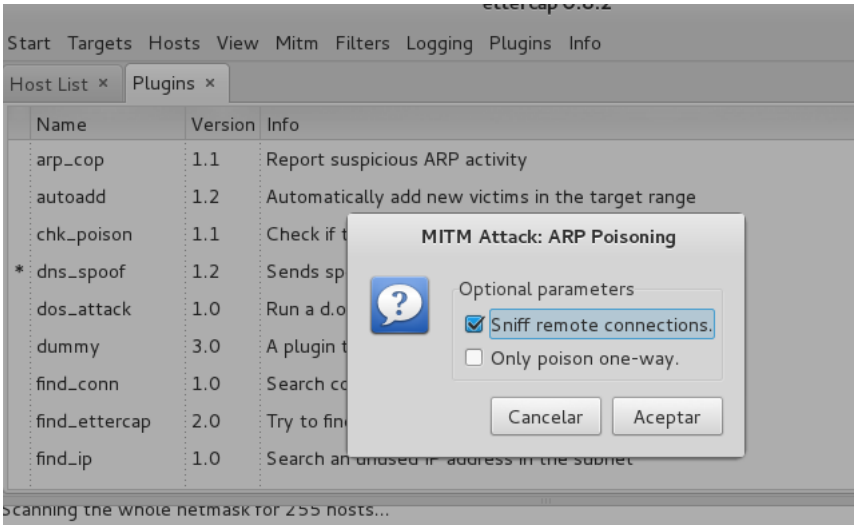

Figura 16: Seleccionado ataque Man in the Middle mediante ARP Spoofing a través de ettercap

Y ya está todo listo. Si la víctima accede al dominio que hemos especificado, ettercap captará la conexión mediante ARP Spoofing y falseará la IP del DNS, devolviendo la IP de nuestro servidor web con el clon. Vamos a verlo:

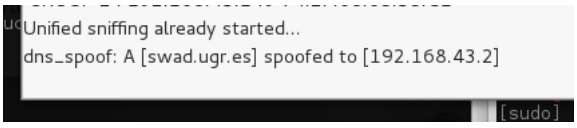

Figura 17: Ettercap redirigiendo el tráfico al atacante

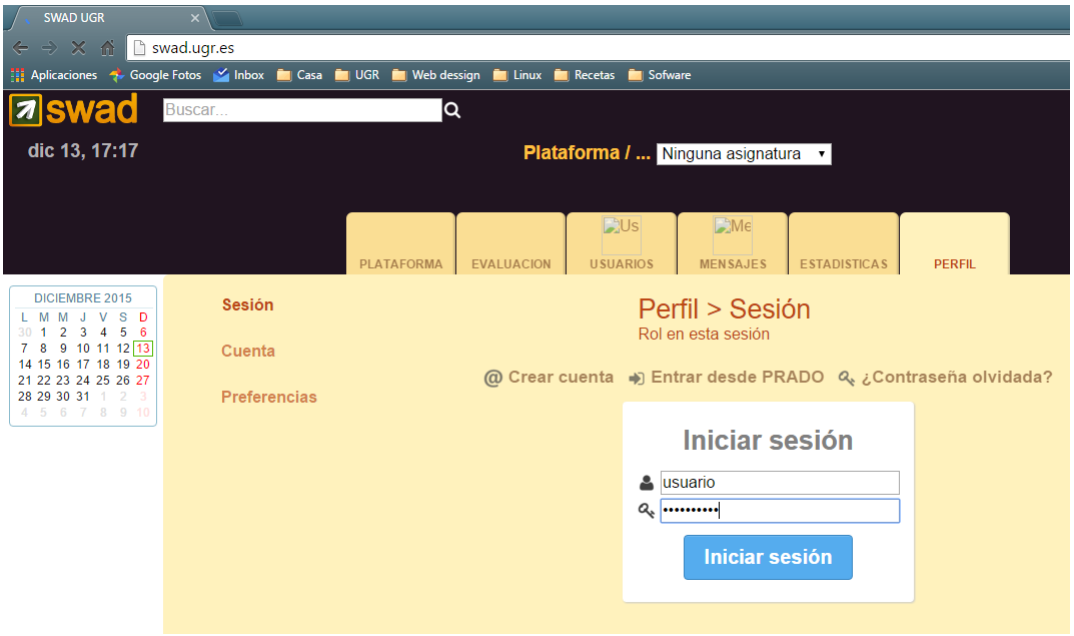

Figura 18: Máquina víctima accediendo al clon de swad

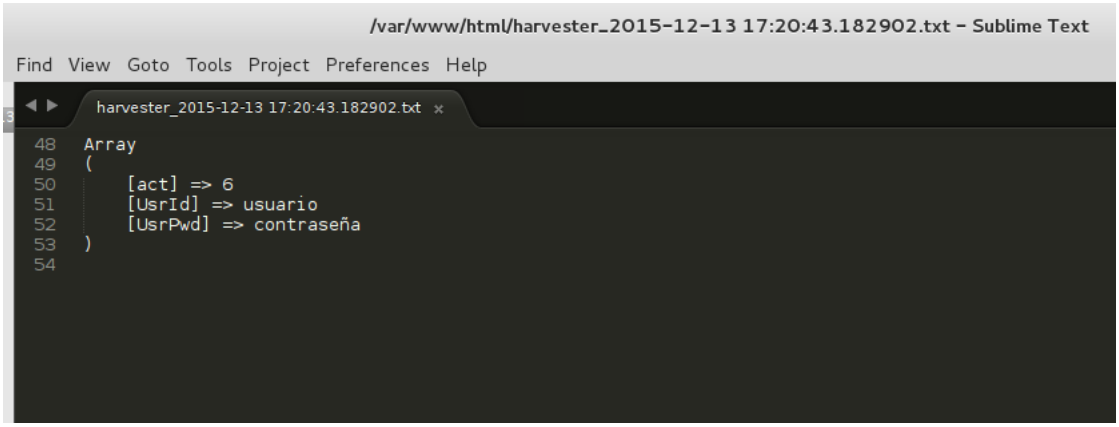

Figura 19: Credenciales de la víctima

Referencias

[1] http://4lfa-om3ga.blogspot.com.es/2012/11/como-detectar-y-evitar-un-arp-spoofing.html, consultado el 12 de Diciembre de 2015.

[2] http://hacking-etico.com/2010/08/26/hablemos-de-spoofing/, consultado el 12 de Diciembre de 2015.

[3] http://onlinelibrary.wiley.com/doi/10.1002/sat.v30.4/issuetoc, consultado el 12 de Diciembre de 2015.

[4] https://en.wikipedia.org/wiki/IP_address_spoofing, consultado el 12 de Diciembre de 2015.

[5] https://en.wikipedia.org/wiki/Spoofing_attack, consultado el 12 de Diciembre de 2015.

[6] https://es.wikipedia.org/wiki/Protocolo_de_resoluci%C3%B3n_de_direcciones, consultado el 12 de Diciembre de 2015.

[7] https://es.wikipedia.org/wiki/Spoofing, consultado el 12 de Diciembre de 2015.

[8] https://es.wikipedia.org/wiki/Web_spoofing, consultado el 12 de Diciembre de 2015.

[9] https://ettercap.github.io/ettercap/, consultado el 12 de Diciembre de 2015.

[10] https://support.google.com/websearch/answer/106318?hl=es, consultado el 12 de Diciembre de 2015.

[11] https://www.infospyware.com/articulos/que-es-el-phishing/, consultado el 12 de Diciembre de 2015.

[12] http://us.wow.com/wiki/Address_resolution_protocolg, consultado el 12 de Diciembre de 2015.

[13] http://www.abc.es/tecnologia/consultorio/20140805/abci-phising-que-es-como-combatirlo-20140805.html, consultado el 12 de Diciembre de 2015.

[14] http://www.e-securing.com/novedad.aspx?id=19, consultado el 12 de Diciembre de 2015.

[15] http://www.mejor-antivirus.es/noticias/gps-spoofing.html, consultado el 12 de Diciembre de 2015.

[16] http://www.pandasecurity.com/spain/homeusers/security-info/cybercrime/phishing/, consultado el 12 de Diciembre de 2015.

[17] http://www.pandasecurity.com/spain/support/card?Id=31442, consultado el 12 de Diciembre de 2015.

[18] http://www.securityartwork.es/2013/09/20/gps-spoofing-i/, consultado el 12 de Diciembre de 2015.

[19] http://www.securityartwork.es/2013/11/22/gps-spoofing-ii/, consultado el 12 de Diciembre de 2015.

[20] http://www.social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set/, consultado el 12 de Diciembre de 2015.

[21] http://www.solution4host.com/wp/how-the-web-spoofing-attack-works/, consultado el 12 de Diciembre de 2015.

[22] http://www.vyaweb.com/preguntas-y-respuestas/que-es-el-spoofing/, consultado el 12 de Diciembre de 2015.

[23] http://www.welivesecurity.com/la-es/2012/06/18/dns-spoofing/, consultado el 12 de Diciembre de 2015.

[24] http://www.wordreference.com/es/translation.asp?tranword=spoof, consultado el 12 de Diciembre de 2015.

[25] http://www.zonavirus.com/articulos/que-es-el-spoofing.asp, consultado el 12 de Diciembre de 2015.