DNS SPOOFING

Autores:

- **Cortés Leyva Carla**
- **Rodríguez padilla Luis**

INDICE

i) DNS

El DNS es una base de datos distribuidas implementadas en una jerarquía de Servidores de nombres y una aplicación de la capa de aplicación que permite que se comuniquen los host y los servidores de nombre para proporcionar el servicio de traducción.

Los servidores de nombres de ejecuta el software de Berkeley Internet Name Domain (BIND). El protocolo DNS se ejecuta sobre UDP y utiliza el puerto 53. Este protocolo funciona entre lados que se comunican utilizando el paradigma cliente-servidor y se basa en un protocolo subyacente de transporte para transferir mensajes DNS entre los sistemas finales comunicantes.

El sistema de dominios asume que todos los datos originados en los ficheros maestros se distribuyen a los hosts del sistema de dominios. Estos ficheros maestros son actualizados por administradores de sistema locales. Los ficheros maestros son ficheros de texto legibles por un servidor de nombres local, y de esta manera se hace disponible desde los servidores de nombres a los usuarios del sistema de dominio. Los programas de usuario acceden a los servidores de nombres a través de programas estándar llamados resolutores. El formato estándar de los ficheros maestros permite que pueda ser intercambiado entre hosts (vía FTP, mail, u otro mecanismo); esta ventaja es útil cuando una organización quiere un dominio, pero no quiere un servidor de nombres. La organización pueden mantener los ficheros maestros de forma local utilizando un editor de texto, enviarlos a un host remoto fuera de la organización que ejecuta un servidor de nombres, y por tanto coordinar con el administrador de sistemas del servidor de nombres para cargar los ficheros. Los servidores de nombres de cada host y los resolutores son configurados por un administrador local de sistemas [RFC-1033]. En cada servidor de nombres, estos datos de configuración incluyen la identidad de los ficheros maestros locales e instrucciones en cada fichero maestro no local para cargarse en servidores fuera de la organización. El servidor de nombres utiliza los ficheros maestros o copias para cargar sus zonas. En el caso de los resolutores, los datos de configuración identifican a los servidores de nombres que deben ser primarios. El sistema de dominio define los procedimientos para acceder a los datos y para referirse a otros servidores de nombres. El sistema de dominio también define los procedimientos para cachear datos y para refrescos periódicos de los datos definidos por el administrador de sistemas.

DNS proporciona otros servicios importantes además de la traducción de nombre de host a direcciones IP: Alias de host: Un host con un nombre complejo puede tener uno o más nombres de alias, los alias de nombre de host son típicamente más mnemotécnicos que los nombres canónicos. El DNS puede ser invocado por una aplicación para obtener el nombre canónico del host y si dirección IP. Alias de Servidor de Correo: Por razones obvias es muy recomendable que las direcciones de correo electrónico sean mnemotécnicas. El DNS puede ser invocado por una

aplicación de correo para obtener el nombre canónico de host a partir del alias proporcionado, así como la dirección IP del host. El registro MX permite que el servidor de correo y el servidor web de una compañía sean nombres de host idénticos. Distribución de carga: Es también utilizado para realizar una distribución de carga entre servidores replicados. La base de datos DNS contiene este conjunto de direcciones IP, cundo un cliente hace una consulta DNS para un nombre que tiene asociado un conjunto de direcciones el servidor responde con el conjunto completo de direcciones IP, pero rota el orden de las direcciones en cada respuesta.

2) DNS SPOOFING

DNS Spoofing o suplantación DNS consiste en un método que utiliza para modificar las direcciones de los servidores DNS que utiliza un usuario.

Los servidores DNS son necesarios para navegar. Actúan como traductores para que, al poner el nombre de dominio, traduzca automáticamente y abra la dirección correspondiente.

Si se modifican esos servidores DNS podría apuntar a una página que no corresponde al poner un nombre de domino. Eso podría pasar con lo que se conoce como DNS Spoofing o suplantación de DNS.

Un atacante puede alterar las direcciones IP de los servidores DNS de la víctima. De esta forma, cuando entra en una página web podría ser redirigido a otra totalmente diferente. Un ejemplo es que escribimos el dominio de una página web de un banco. En caso de que hayan realizado un ataque DNS Spoofing podrían redirigir a una web que simule ser la del banco, con el objetivo de llevar a cabo un ataque Phishing y recopilar las contraseñas.

La forma en la cual esto es realizado es de la siguiente manera:

El usuario realiza una solicitud a un servidor DNS para que resuelva un nombre de dominio, como podría ser redeszone.net. Sin embargo, en caso de ser víctimas de este ataque, ese servidor DNS nos va a dar una respuesta que nos dirige a un sitio ilegítimo, en vez de al que esperamos entrar.

En esta imagen mostramos básicamente como funciona un DNSspoof.

2) HERRAMIENTAS

En esta práctica, se busca la realización de un DNS spoofing, apoyándonos de apache 2, setoolkit y ettercap .

i) APACHE2

(a) ¿QUÉ ES?

Es un servidor web http de código abierto, para plataformas unix microsoft windows, macintosh y otras, que implementa el protocolo HTTP/1.1 y la noción de sitio virtual según la normativa RFC 2616.

El servidor Apache es desarrollado y mantenido por una comunidad de usuarios bajo la supervisión de la Apache Software Foundation dentro del proyecto HTTP Server (httpd).

Apache presenta entre otras características altamente configurables, bases de datos de autenticación y negociado de contenido, pero fue criticado por la falta de una interfaz gráfica que ayude en su configuración.

La mayoría de las vulnerabilidades de la seguridad descubiertas y resueltas tan solo pueden ser aprovechadas por usuarios locales y no remotamente. Sin embargo, algunas se pueden accionar remotamente en ciertas situaciones, o explotar por los usuarios locales maliciosos en las disposiciones de recibimiento compartidas que utilizan PHP como módulo de Apache.

(b) USOS

Apache es usado principalmente para enviar páginas web estáticas y dinámicas en la World Wide Web. Muchas aplicaciones web están diseñadas asumiendo como ambiente de implantación a Apache, o que utilizarán características propias de este servidor web.

Apache es usado para muchas otras tareas donde el contenido necesita ser puesto a disposición en una forma segura y confiable. Un ejemplo es al momento de compartir archivos desde una computadora personal hacia Internet. Un usuario que tiene Apache instalado en su escritorio puede colocar arbitrariamente archivos en la raíz de documentos de Apache, desde donde pueden ser compartidos.

Los programadores de aplicaciones web a veces utilizan una versión local de Apache con el fin de previsualizar y probar código mientras este es desarrollado.

ii) ETTERCAP

(a) ¿QUÉ ES?

Ettercap es un interceptor/sniffer/registrador para LANs con switch. Sirve en redes LAN conmutadas, aunque es utilizado para auditorías en distintos tipos de redes.

Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo aun manteniendo la conexión sincronizada gracias a su poder para establecer un Ataque Man-in-the-middle(Spoofing). Muchos modos de sniffing fueron implementados para darnos un conjunto de herramientas poderoso y completo de sniffing. Además, es capaz de revisar y analizar si se trata de una red LAN con "switch" o no e incluye detección remota de OS

iii) SETOOLKIT

SET es una completísima suite dedicada a la ingeniería social , que nos permite automatizar tareas que van desde el de envío de SMS (mensajes de texto) falsos, con los que podemos suplantar el número telefónico que envía el mensaje, a clonar cualquier página web y poner en marcha un servidor para hacer phishing en cuestión de segundos.

El kit de herramientas SET está especialmente diseñado para realizar ataques avanzados contra el elemento humano. Originalmente, este instrumento fue diseñado para ser publicado con el lanzamiento de http://www.social-engineer.org y rápidamente se ha convertido en una herramienta estándar en el arsenal de los pentesters. SET fue escrito por David Kennedy (ReL1K) con un montón de ayuda de la comunidad en la incorporación de los ataques nunca antes vistos en un juego de herramientas de explotación.

3) PRACTICA

En esta practica se busca la realización de un ataque DNS Spoof, el cual será explicado detalladamente a continuación.

Esta práctica se trabajo principalmente con una maquina Kali Linux que es la atacante, su IP es: 192.168.1.83.

Lo primero que se realizo fue la instalación de las herramientas con las que trabajaremos:

- Sudo apt-get install apache2

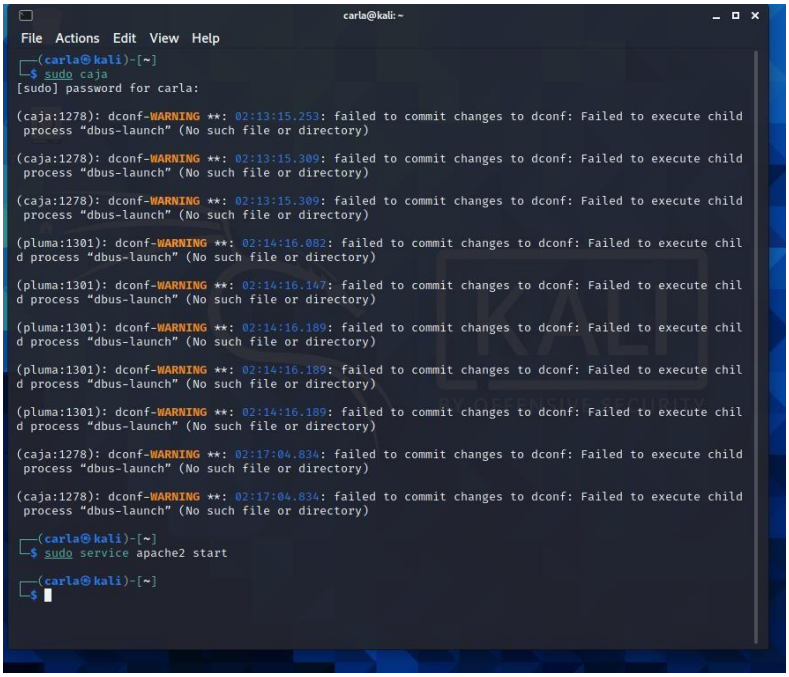
Procederemos a iniciar el apache2con el siguiente comando:

- sudo service apache2 start (si se desea detener se cambia el start por stop).

Recordando que la herramienta apache2 solo puede ser utilizada en en la maquina que se esta ejecutando y para permitir que este sea visto por los demás dispositivos conectados a nuestra red. Mediante el siguiente comando descargaremos y gestionaremos el firewall, permitiremos el trafico entrante en el puerto 80:

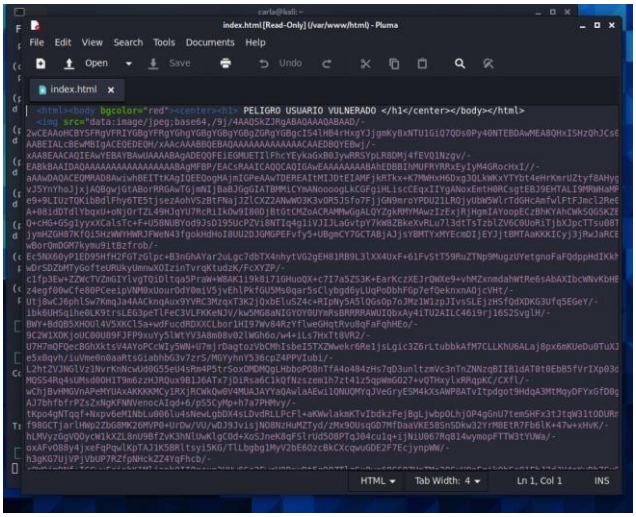
- Sudo apt-get install ufw

- Sudo ufw allow 80 (para cancelarlo se cambia el allow por deny)



(En esta imagen se muestra como iniciamos apache2)

Procedemos a editar página generada en apache2 la cual se encuentra en nuestro File System, en una carpeta llamada Var, ahí encontraremos una carpeta llamada WWW y entrando en ella encontraremos una carpeta llamada HTML, ahí encontraremos el archivo index que editaremos para poder darle formato a nuestra página.



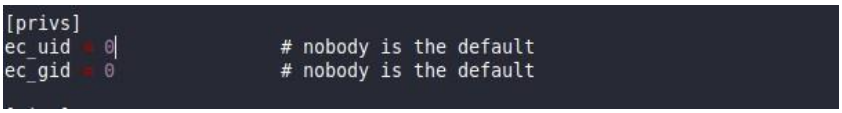
Con el apache iniciado procederemos a descargar la segunda herramienta con la que trabajaremos que es ettercap de la siguiente forma:

- Sudo apt-get install ettercap -graphical

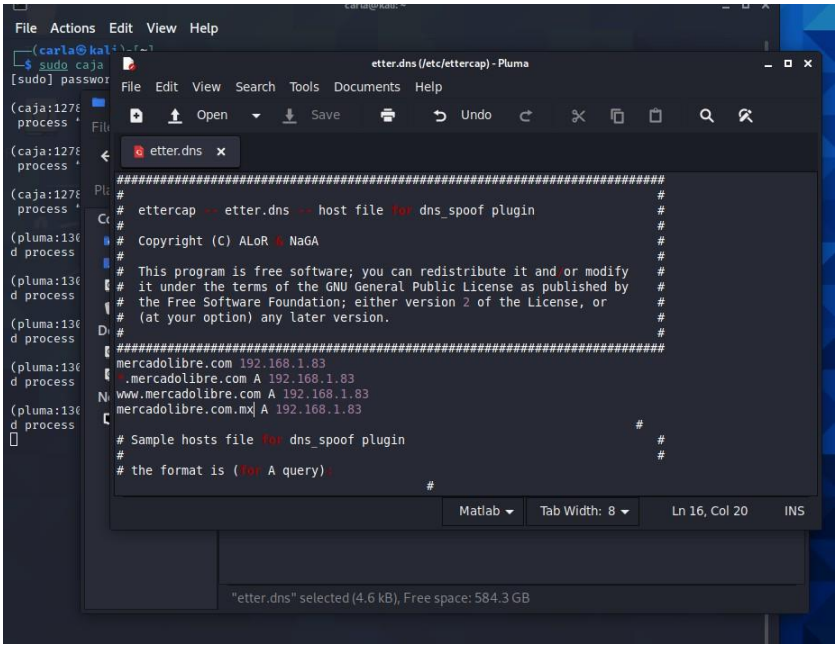
Ettercap funcionara como nuestro servidor DNS.

Al descargar ettercap ahora debemos editar dos carpetas que nos van a permitir redireccionamiento a nuestro IP, para acceder a estar carpetas lo haremos nuevamente desde nuestra terminal/FILE System, encontraremos una carpeta con el nombre de etc, al abrirla debemos buscar la carpeta ettercap en la cual editaremos dos archivos:

El primero es el archivo llamado etter.conf en el cual realizaremos un cambio que nos permitirá ejecutar el programa como root igualando a 0 como se muestra a continuación

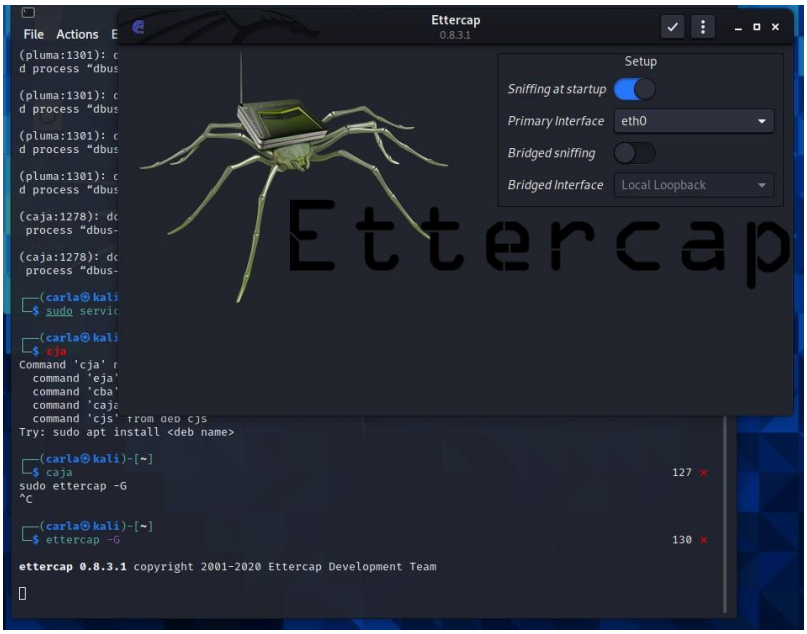


A continuación editaremos un segundo archivo que encontramos con el nombre de etter.dns en el cual indicaremos la página que suplantaremos y hacia donde redireccionaremos, en este caso seleccione mercado libre. Significando que cuando el usuario de la maquina vulnerada decida abrir mercado libre sera enviado a la página que fue editada al principio de la practica

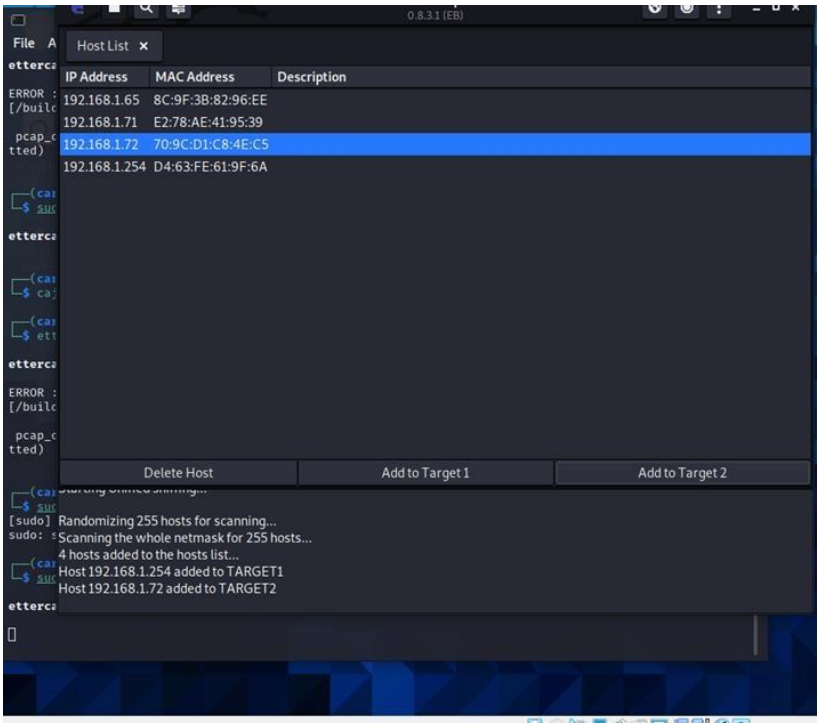


Ahora iniciaremos el ataque echando a andar la herramienta ettercap con el siguiente comando:

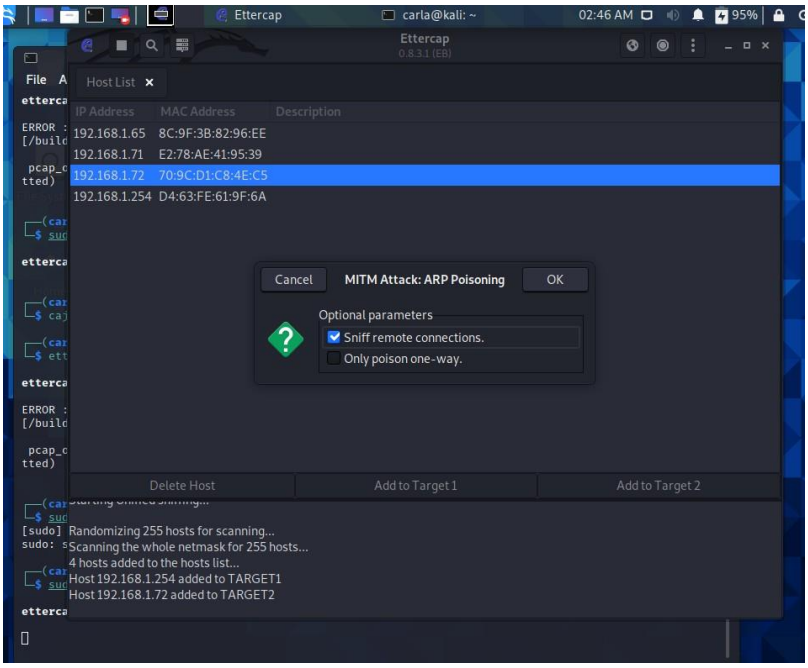
- Sudo ettercap -G



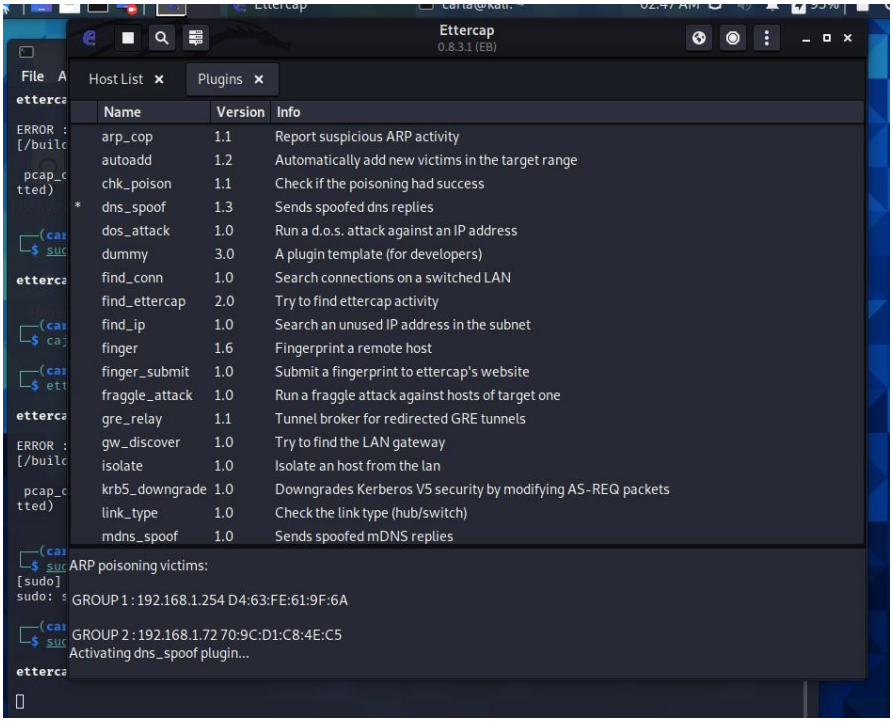
Ahora en ettercap podemos escanear los dispositivos que se encuentran en nuestra red y seleccionamos a cuáles se les realizara el ataque, en este caso el ip de mi maquina es 192.168.1.72



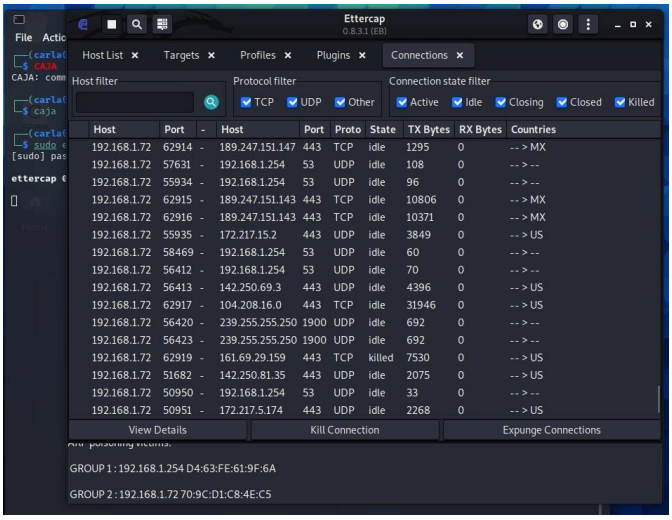
Continuamos configurando nuestro ataque seleccionando la opción que se muestra en la siguiente imagen, la cual nos permitirá observar el flujo de datos en las conexiones remotas.



En el apartado pluggins encontramos todos los ataques con los que podemos trabajar en ettercap, en este caso seleccionamos dns_spoof

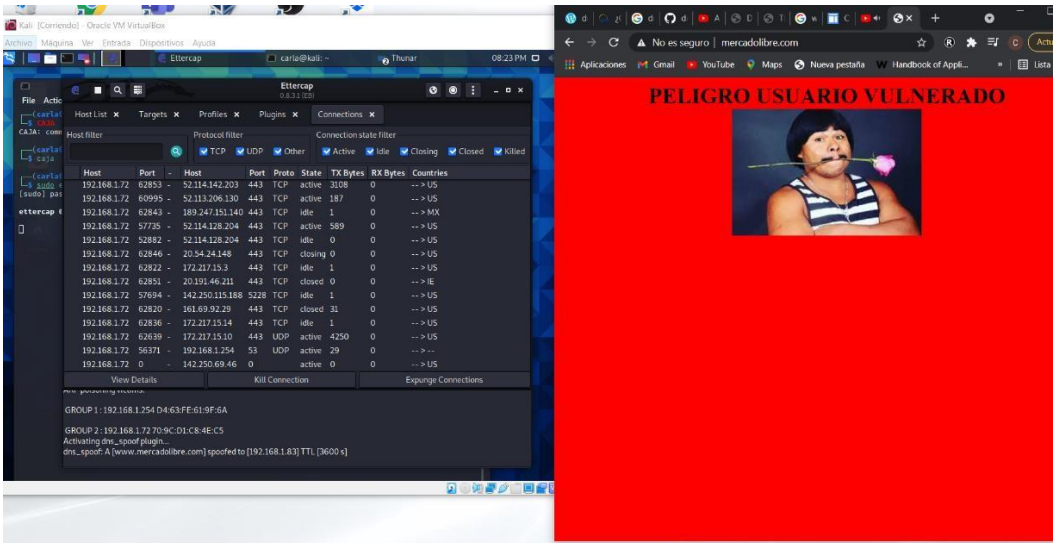


Y nos damos cuenta que podemos observar el tráfico y todo lo que el usuario al cual realizaremos el ataque se encuentran haciendo (es este caso las páginas que está ocupando), en este punto solo queda probar si nuestro ataque resulto de la forma que deseamos



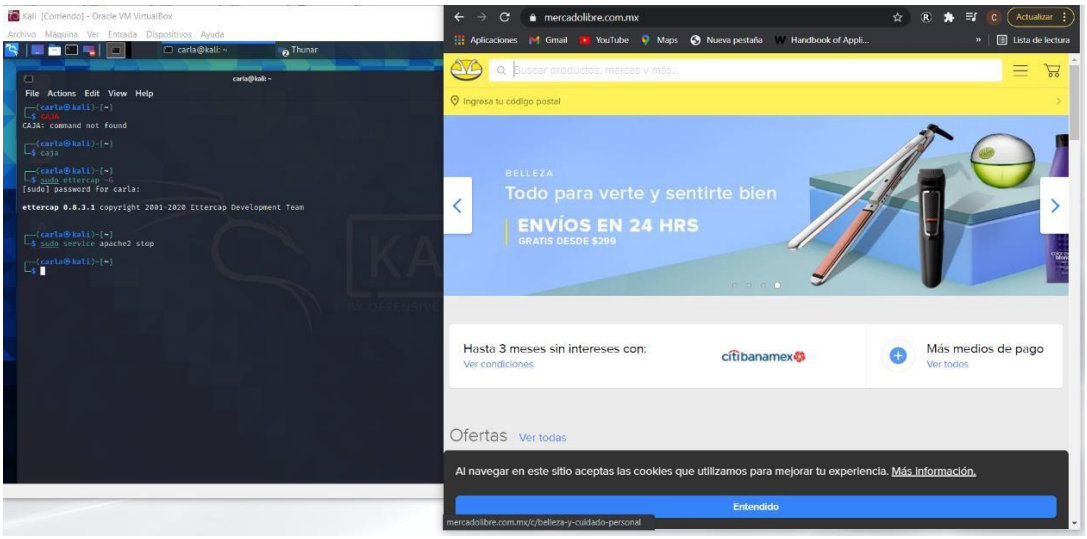
Y desde la maquina a la cual se realiza el ataque intentamos abrir mercadolibre.com.

Como se puede observar en la siguiente imagen nuestro ataque tuvo éxito ya que al momento que se intentó abrir mercadolibre.com fuimos redireccionando a la página que creamos.

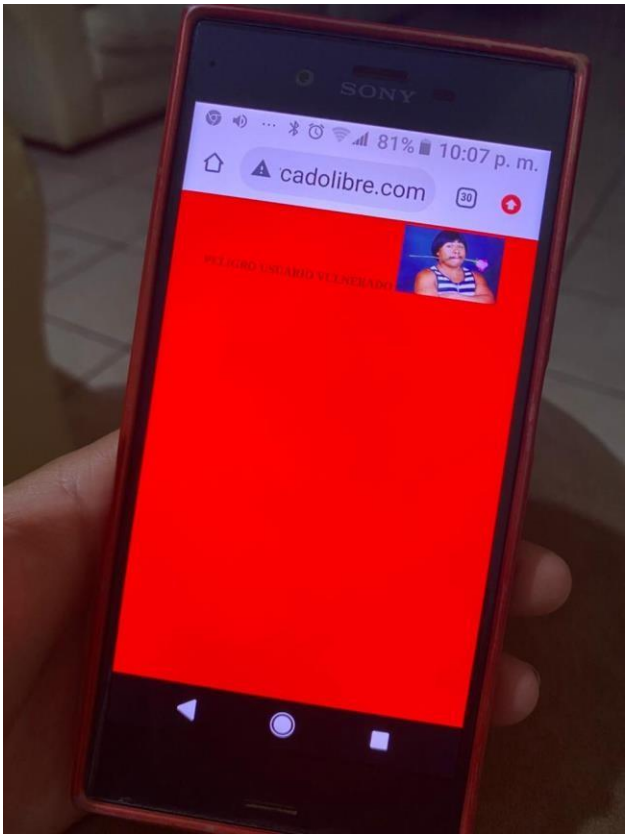


Al obtener el éxito esperado, terminamos deteniendo nuestras herramientas utilizadas para realizar este ataque y nuevamente intentamos abrir la pagina a la

redireccionamos y podemos observar que nos permite ingresar sin problema alguno.



Incluso la práctica se puede aplicar a algunos dispositivos en nuestra red, podemos observar que el redireccionamiento fue correcto.



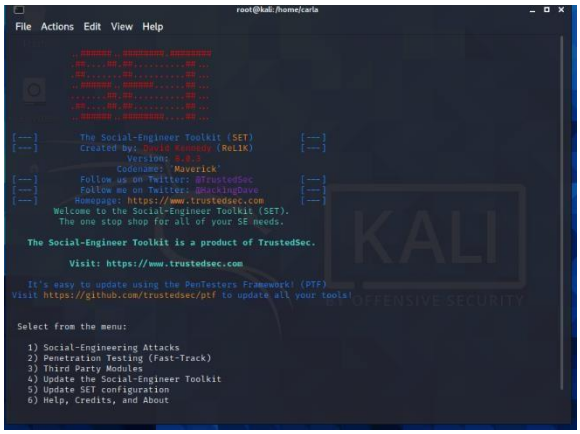
ii)DNS SPOOFING SUPLANTACION DE IDENTIDAD DE UN SITIO WEB

En este ejemplo estaremos trabajando con una máquina virtual Kali Linux y una maquina Windows 7.

Para este ejemplo utilizaremos nuevamente la herramienta ettercap y nuevamente configuraremos las carpetas, en este caso yo cambien la página a la cual suplantaríamos que es Facebook.com y redireccione a la ip de mi maquina atacante.

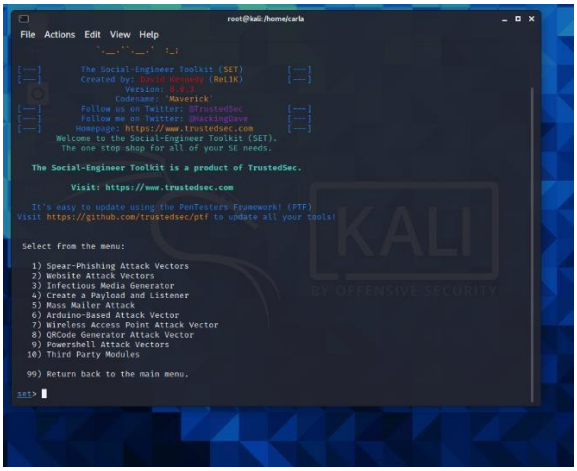
De esta forma estamos envenenando las consultas DNS.

A continuación, procederemos ejecutando setoolkit, la cual ejecutaremos como super usuarios y nos desplegara el menú de inicio el cual luce de la siguiente manera:

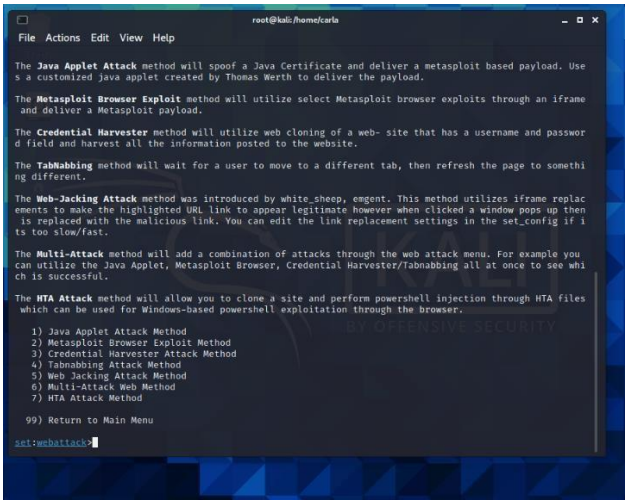


y procederemos a seleccionaremos las primer opción 1)Social-Engineering Attacks

La cual nos mandara a un segundo menú en el cual seleccionaremos la opción numero 2)Website Attack Vectors



Llegaremos a un 3er menú en el cual seleccionaremos la opción numero 3)Credential Harvester Attack Method



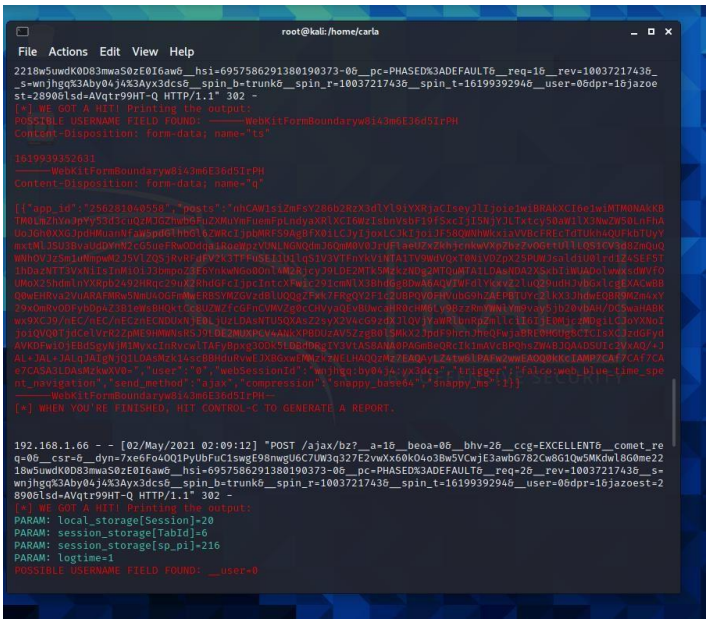
El cual nos mandara al último menú en el cual realizaremos la copia de la página asi que seleccionaremos la opcion 2)Site Cloner.

Nos pedira que ingresemos el ip que deseamos sea asigando a nuestra copia.

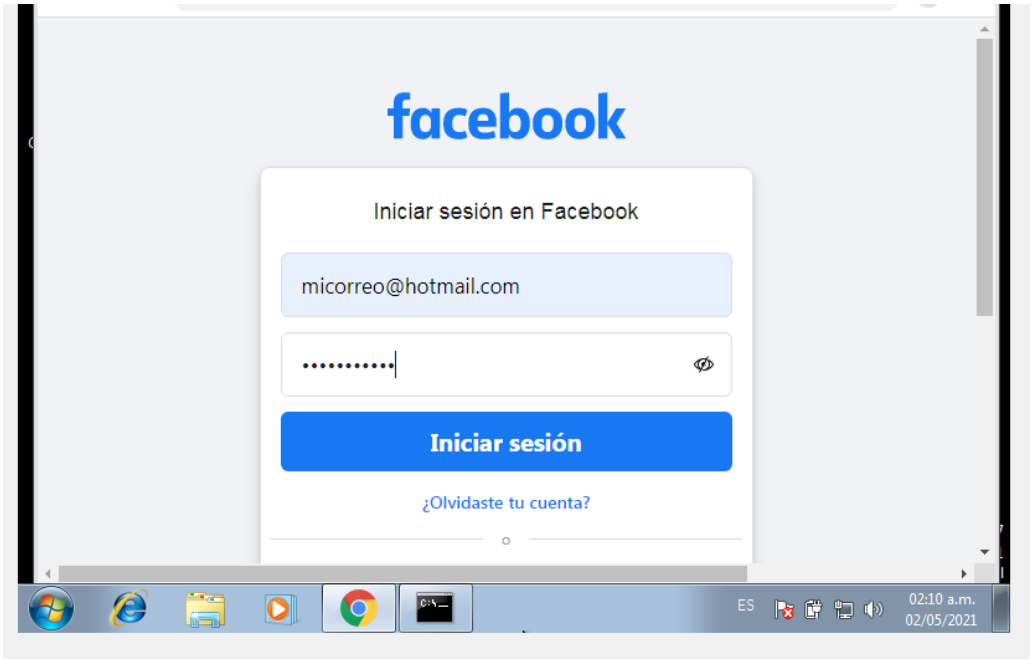
Y como se muestra en la siguiente imagen, ingresaremos el url a clonar

Mediante Ettercap nosotros seleccionaremos el ip del disposito al cual atacaremos e iniciaremos el ataque dns_spoof, y comienza el ataque.

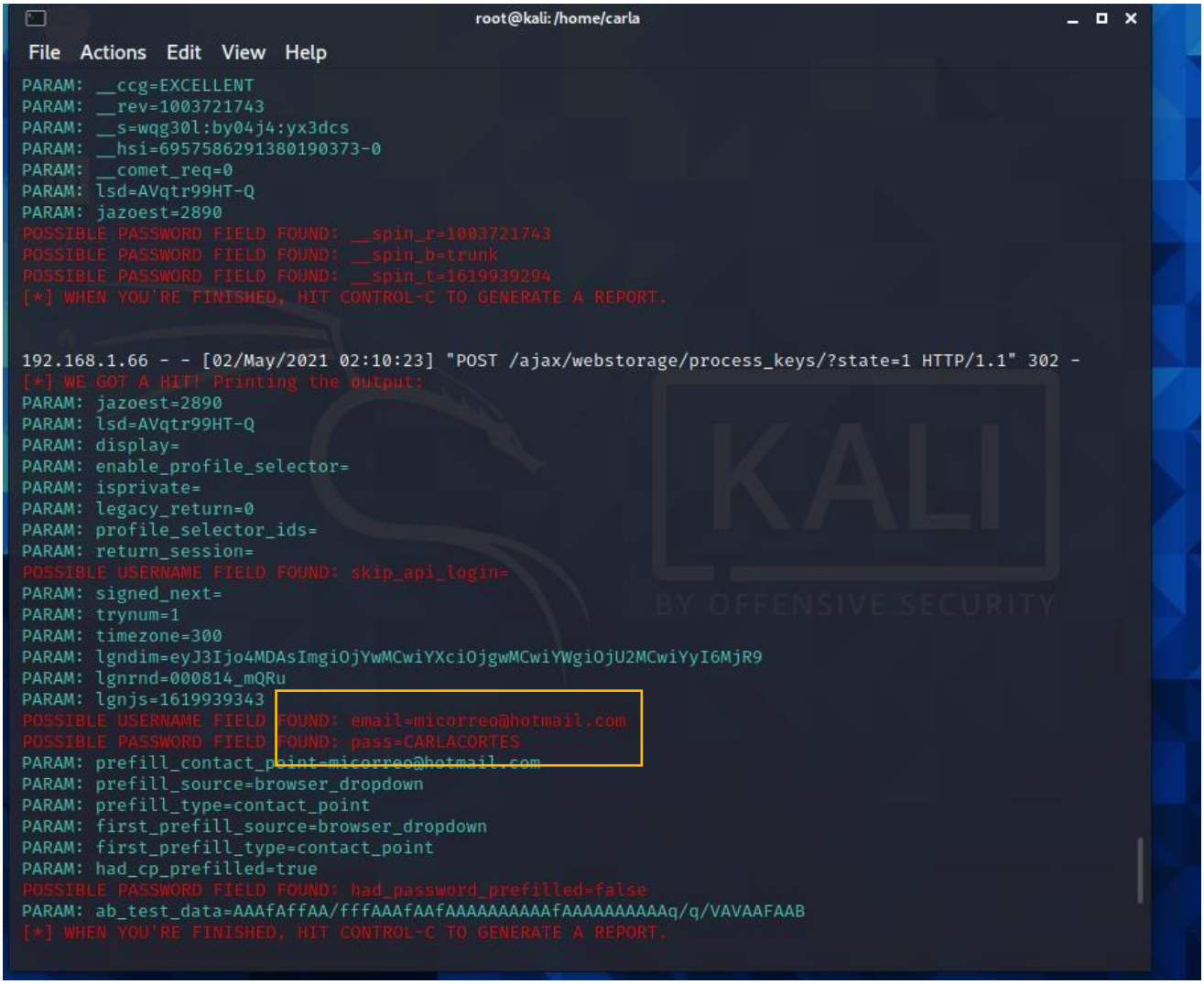
Desde la windows 7 procederemos a abrir www.facebook.com y podemos notar como inmediatamente tenemos respuesta en la maquina atacante informándonos que la maquina atacada ingreso a nuestra copia



El usuario ingresa sus datos como normalmente lo haría para poder ingresar a su cuenta sin saber lo que está sucediendo, y al momento que el intenta iniciar sesión, la página vuelve a cargar, de esta forma él puede llegar a creer que tal vez su internet fallo o ingreso mal sus datos, la segunda vez que el ingresa sus datos ahora si puede acceder de forma correcta a la página facebook, pero…..



El no contempla que lo sucedido anteriormente fue un ataque, y ese pequeño problema al cual no le tomo importancia permite al atacante robar su información, en este caso usuario y contraseña.



Si nos detenemos a revisar el análisis de nuestra red podemos observar lo siguiente.

Desde nuestra maquina windos 7 (en este caso la maquina atacada) jamás tuve algún tipo de aviso sobre que nos encontrábamos bajo ataque hasta que abrí el wireshark y pude notar inconsistencias en mi red como por ejemplo podemos encontrar TCP retransmission, este mecanismo de retransmisión de TCP garantiza que los datos se envíen de forma fiable de un extremo a otro y aquí podemos notar que nos está indicando que se ha producido una pérdida de paquetes en la red entre el cliente y el servidor

REFERENCIAS

- Br. José Rodolfo Herrera Baca, GUIA PRACTICA DE ATAQUES DE SPOOFING, DoS E INYECCIONES SQL Y SUS POSIBLES SOLUCIONES, [tesis, Universidad Nacional Autónoma de Nicaragua. UNAN-León]
- Welcome! - The Apache HTTP Server Project
- https://www.ettercap-project.org/
- https://github.com/trustedsec/social-engineer-toolkit
- AFF741E8-BDC9-473C-A235-2B5E5AD4E00A.pdf RFC 1034
- E4F2B534-BDB7-44FC-8BD2-6329897B4C5A.pdf RFC 1035
- https://www.welivesecurity.com/la-es/2017/02/09/ataques-al-dns/