Ataque a servidores DNS

A continuación se procede a exponer los principales ataques a servidores DNS con algún que otro caso práctico. Para realizar las pruebas se ha utilizado la suite de herramientas ADM (incluida en backtrack 4) de la cual veremos las más interesantes. Como servidor DNS se ha utilizado Bind.

Podemos dividir los principales ataques en dos categorías:

1.- DoS (*Denial of Service*)

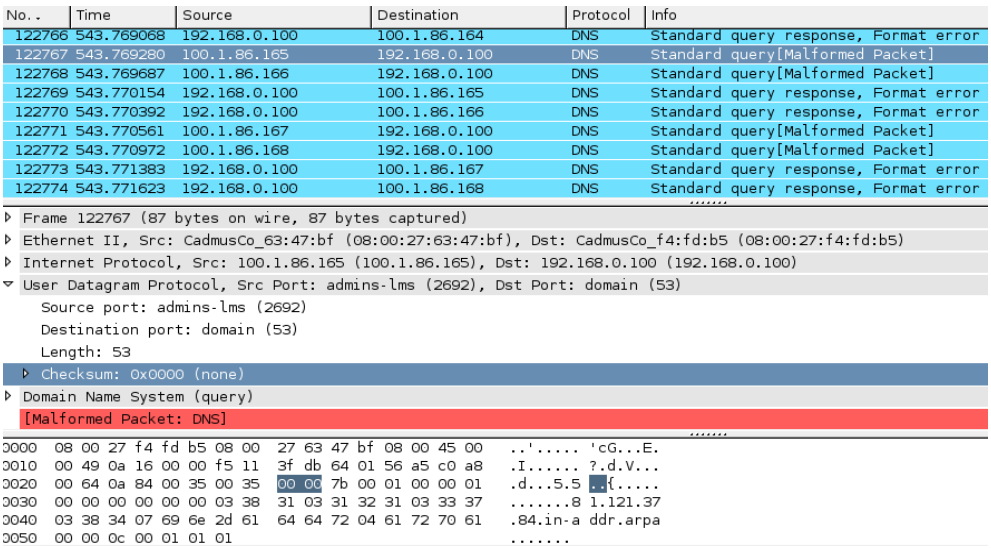
Como su propio nombre indica, estos ataques consisten en impedir que los usuarios utilicen el servicio. Nos centraremos en el ataque al ancho de banda. Veamos como abordarlo con *ADMdnsfuckr*.

1.1.- ADMdnsfuckr

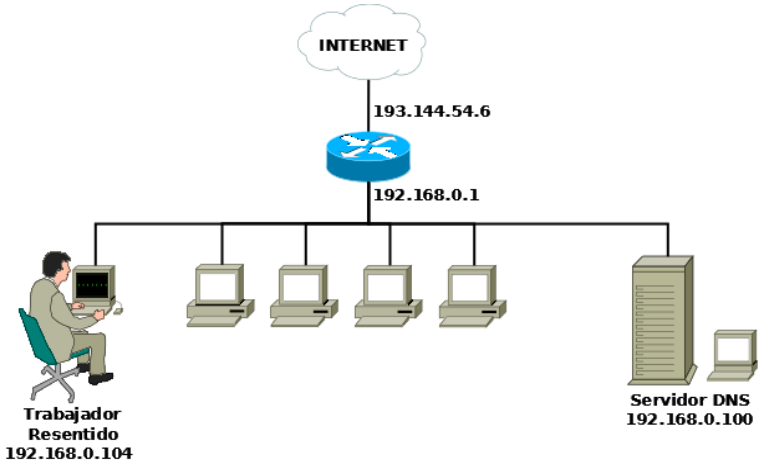
```
# ADMdnsfuckr 192.168.0.100
```

Argumentos: IP destino

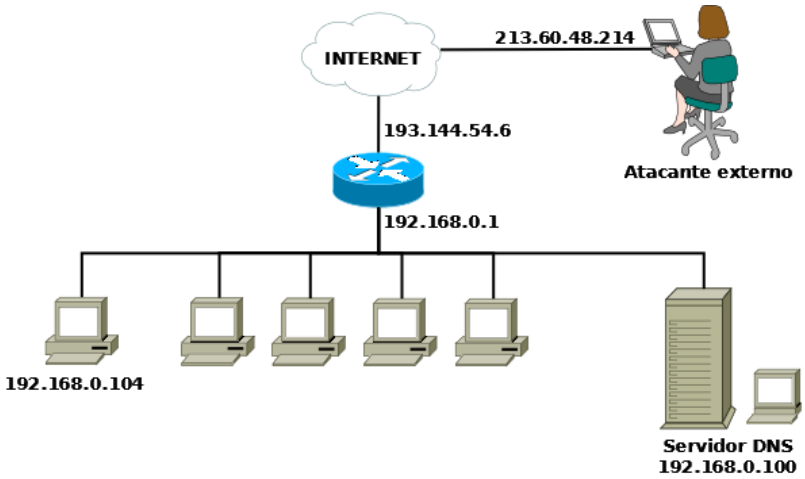
La aplicación manda múltiples peticiones PTR (resolución inversa IP → dominio) de IPs aleatorias al servidor DNS. Para ello realiza un par de cambios en los paquetes. Por un lado cambia la IP origen (una para cada paquete) empezando siempre en 100.1.10.0 (que es un rango de IPs de las que no se usan). Por otro lado modifica el checksum de la cabecera UDP poniéndolo a 0000, entonces manda paquetes erróneos. Como son erróneos el servidor debería mandar la respuesta correspondiente a cada error.



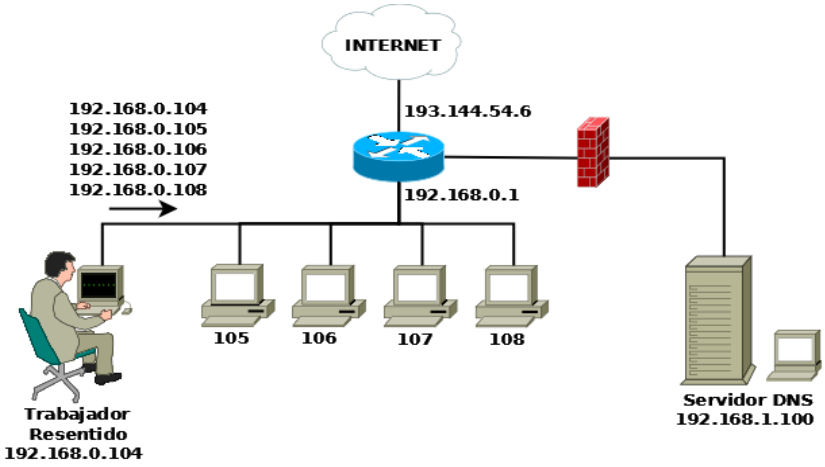
Es fácil ver que las pruebas están realizadas sobre un DNS que está en el mismo segmento de red.



Dicho esto y dependiendo de la complejidad del servidor DNS pueden pasar dos cosas: que el servidor trague y responda a cada una de las peticiones o bien que las interprete y no las responda (lo que no impide que el ataque pueda ser satisfactorio). No obstante lo habitual suele ser que el DNS no esté en nuestro propio segmento de red, por ejemplo en una gran organización o si simplemente el atacante es externo.



De esta manera al estar fuera del segmento existe una gran probabilidad de que el activo de red tire la paquetería, y si hay un firewall de por medio seguro que la tira. Entonces si tenemos un firewall sólo queda una opción. Si volvemos al caso del “Trabajador resentido” este podría spoofear con IPs del segmento.



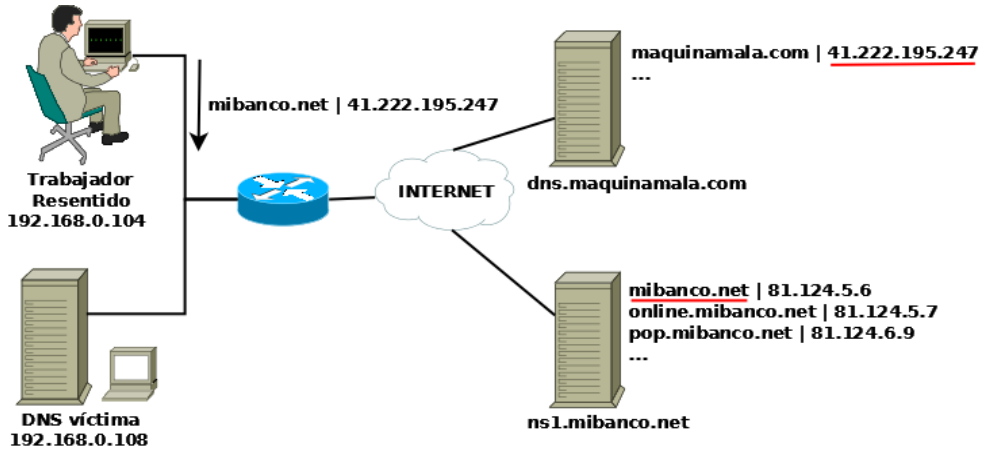
Ahora aunque acotado en posibilidades el ataque sería efectivo ya que el servidor tiene que responder las peticiones de ese segmento. Lo único que se podría hacer sería tomar medidas como limitar el número de conexiones o reducir el ancho de banda con determinadas IPs dado que se está atacando con IPs de máquinas comprometidas a las que no se les puede negar el servicio. Claro que si el firewall del segmento evita el spoofing no se conseguirá nada.

2.- DNS Spoofing

Suplantación de identidad por nombre de dominio. 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. Dentro del DNS Spoofing podemos subdividir en ataques de TXID (o envenenamiento de la caché) y los MitM (Man in the Middle). Aunque los últimos no van dirigidos directamente contra el servidor, suplantan las peticiones contra el mismo. Como es obvio, todos estos sufren los mismos problemas de eficacia en función de la ubicación del origen y el destino, así como de la existencia de firewalls al igual que hemos visto en el caso del DoS en cuanto a suplantación se refiere.

2.1.- TXID

Un DNS utiliza un ID aleatorio para sus paquetes, pero esto solo es en la primera consulta, después lo incrementa para las sucesivas consultas de forma que si es posible esnifar el DNS se puede predecir el ID. En anteriores versiones de Bind esto permitía suplantar a un DNS autoritario sobre un DNS víctima y así modificar su caché a voluntad.



Las versiones de Bind anteriores a la 8.4.7 tienen este problema, aunque actualmente todos los DNS están actualizados o parcheados (o al menos deberían). Llegados a este punto puede ser interesante analizar el grado de vulnerabilidad de un servidor DNS. Si utilizamos el nmap con el script dns-random-txid lo podemos analizar:

```
# nmap -sU --script=dns-random-txid 192.168.0.108 -p 53

Starting Nmap 5.00 ( http://nmap.org ) at 2010-04-02 20:22 CEST
Interesting ports on 192.168.0.108:
PORT   STATE SERVICE
53/udp open  domain
|_ dns-random-txid: 192.168.0.108 is GREAT: 26 queries in 4.7 seconds from 26 txids with std dev
19069
```

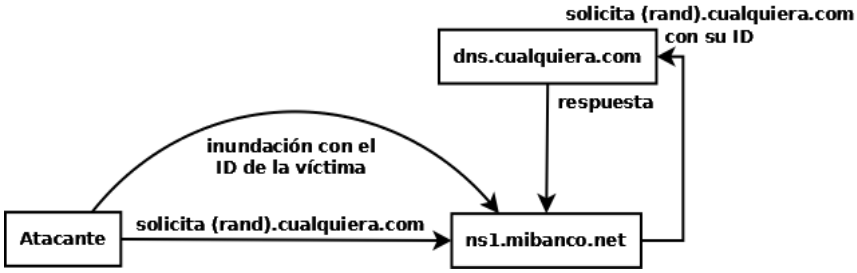
Nos encontramos que la aleatoriedad es estupenda (GREAT), en caso contrario, el servidor sería vulnerable.

Vamos a ver el funcionamiento de dos de las herramientas de ADM, ADMsnOOfID y ADMnOg00d.

2.1.1.- ADMsnOOfID

```
# ADMsnOOfID eth0 192.168.0.108 cualquiera.com dns.cualquiera.com 1 mibanco.net 41.222.195.247
ns1.mibanco.net
```

Argumentos: interfaz | DNS víctima | un dominio cualquiera | DNS con autoridad en el dominio anterior | tipo de petición DNS 1 o 12 (A o PTR) | dominio spoof | ip spoof | DNS con autoridad en el dominio o en la ip de spoof



Para poder hacer uso de esta aplicación hay que tener en cuenta que se necesita un DNS con autoridad sobre un dominio y que podamos esnifar sus mensajes. Un ejemplo claro sería tener ese DNS en nuestro segmento de red o bien el DNS víctima. Secuencia que seguiría la aplicación:

- Esnifar los mensajes de un DNS cualquiera (dns.cualquiera.com).
- Preguntar a la víctima (ns1.mibanco.net) para que resuelva (rand).cualquiera.com (4h1qak.cualquiera.com por ejemplo). En este momento ya tendríamos el ID actual del DNS víctima y podemos utilizarlo para envenenar la caché con los pares dominio-ip que queramos.
- El Atacante manda la resolución para el envenenamiento (mibanco.net | 41.222.195.247) incrementando el ID anterior mediante inundación.

```
kewl :)~ we have the packet !
the current id of 192.168.0.108 is 13994
send the spoof...
trustip    81.124.5.6,vitcimip    192.168.0.108,spoofna    mibanco.net,spoofip    41.222.195.247,ID
13994,type 1 I apres Makepaket == 34
trustip    81.124.5.6,vitcimip    192.168.0.108,spoofna    mibanco.net,spoofip    41.222.195.247,ID
13995,type 1 I apres Makepaket == 34
trustip    81.124.5.6,vitcimip    192.168.0.108,spoofna    mibanco.net,spoofip    41.222.195.247,ID
13996,type 1 I apres Makepaket == 34
trustip    81.124.5.6,vitcimip    192.168.0.108,spoofna    mibanco.net,spoofip    41.222.195.247,ID
13997,type 1 I apres Makepaket == 34
```

- La víctima tiene ahora el par dominio-ip como una entrada legal y todas las máquinas que accedan a consultarle lo recibirán como respuesta.

2.1.2.- ADMnOg00D

```
#  ADMnOg00d  192.168.0.111  dns.cualquiera.com  cualquiera.com  192.168.0.108  1  mibanco.net
41.222.195.247 ns1.mibanco.net 2012
```

Argumentos: tu ip | un DNS cualquiera | dominio en el DNS anterior | DNS víctima | tipo de petición DNS 1 o 12 (A o PTR) | dominio spoof | ip spoof | DNS con autoridad en el dominio o en la ip de spoof | ID para el DNS

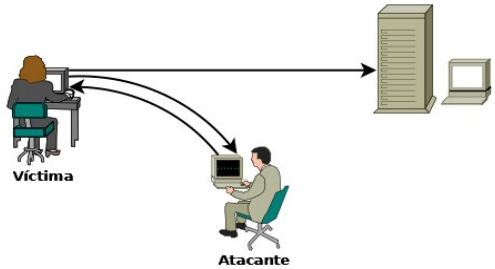
Esta aplicación es idéntica a la anterior (ADMsnOOfID) aunque está orientada al caso de no poder esnifar el tráfico para coger el ID de la víctima, por lo que mediante fuerza bruta averigua el ID. Aunque es más lento, no deja de ser efectivo. Para ello se le pasa un número de ID a la aplicación y este se va decrementando hasta encontrar el adecuado.

```
try 2002 < ID < 2012
ok whe have the reponse ;)
fakename = 44478614975118.cualquiera.com
try 1991 < ID < 2001
ok whe have the reponse ;)
fakename = 483514351106142.cualquiera.com
try 1980 < ID < 1990
ok whe have the reponse ;)
fakename = 4414568881632.cualquiera.com
try 1969 < ID < 1979
ok whe have the reponse ;)
fakename = 4812813115070108.cualquiera.com
try 1958 < ID < 1968
ok whe have the reponse ;)
fakename = 17122611780.cualquiera.com
try 1947 < ID < 1957
ok whe have the reponse ;)
fakename = 1476693810534.cualquiera.com
…
```

Sin embargo esta aplicación tiene un problema, genera mucho tráfico y sería posible una rápida actuación por la parte atacada a consecuencia.

2.2.- MitM

Los ataques Man in the Middle (o intermediario) son ataques contra el flujo de la información entre dos máquinas. El atacante lee y modifica la información del flujo sin que se percaten las máquinas afectadas. Para el caso del DNS, el atacante esnifa las peticiones DNS de la víctima y las responde haciéndose pasar por el servidor DNS que utiliza la víctima.



Para este tipo de ataques la suite ADM tiene dos aplicaciones pero es suficiente con decir que están ahí ya que hay otras mucho más versátiles y desarrolladas como ettercap. Dejo como sugerencia al lector el estudio del ettercap por su cuenta ya que hay mucha documentación por la red.