



Published on hacktimes.com (<http://www.hacktimes.com>)

Fingerprinting de DNS con FPDNS

By vaxman

Creado 9 Jan 2006 - 10:50

La manera más eficaz de obtener información en una auditoria de seguridad es hacer un reconocimiento de los sistemas operativos y servicios instalados en el sistema que se va a revisar, esta técnica se denomina **fingerprinting**.

Saber las versiones de los programas utilizados para implementar los servicios es fundamental para conocer con exactitud qué vulnerabilidades se pueden utilizar contra ellos. Con el nombre del programa y la versión, una simple búsqueda en Bugtraq www.securityfocus.com [1] o en cualquier buscador de vulnerabilidades nos permitirá obtener los fallos publicos que afectan a dicho programa.

La forma más fácil, y también la menos fiable, de reconocer un programa y su versión es capturando el banner que proporciona el servidor al hacerle una petición. En el caso de un servicio DNS existen diferentes formas de ofuscar e incluso impedir el proporcionar información acerca del software instalado y de su versión, ya sea con el programa BIND, eNom, Windows, ATLAS, o cualquier otro software de DNS utilizado.

Para hacer fingerprinting de un servicio DNS existe una herramienta que aún es poco conocida pero que es sumamente fiable, denominada fpdns [2] de los autores **Roy Arends y Jakob Schlyter** que detecta remotamente los programas servidores DNS realizando peticiones en busca de diferentes implementaciones del protocolo características de los distintos fabricantes.

Se trata de un script en perl que como único requisito necesita disponer de la última versión de Net::DNS, www.net-dns.org [3], muy fácil de usar y con numerosas opciones útiles. El funcionamiento es sumamente sencillo ya que se basa en realizar diversas peticiones específicas en busca del programa y la versión del software DNS que hay en el servidor, dado que la respuesta es diferente en función del programa DNS utilizado, no resulta complicado el poder establecer un muestreo bastante veraz del software DNS que está instalado en el "nameserver".

Sólo se han detectado problemas de falsos positivos o errores en el reconocimiento, tal y como explican sus autores en la página Web <http://www.rfc.se/fpdns/>, ante sistemas balanceados o detrás de algún firewall que no funciona con el estandar "statefull inspection" de CheckPoint, actualmente, presente en todos los sistemas de firewall (Cisco Pix, FW-1, Stonegate, etc).

En la página de los autores se puede obtener un extenso listado de todos los programas que es capaz de reconocer y entre ellos se encuentra el archiconocido y utilizado BIND (en todas sus versiones) que es el que se encuentra instalado en un 80% de los servidores de DNS de Internet.

Las opciones más destacables que presenta `fpdns.pl`son:

- `d` (para activar el modo debug y comprobar qué tipo de peticiones se hacen en cada momento).
- `v` (para mostrar la versión del `fpdns` que se está ejecutando).
- `r n°_intentos` (para permitir al `fpdns` reintentar X veces la petición DNS).
- `t n°_timeout` (para modificar el timeout en las peticiones DNS).
- `p n°_puerto` (para modificar el puerto UDP en el que está escuchando el servicio DNS analizado).
- `Q dirección_IP_origen` (para establecer desde qué dirección IP se realiza el análisis del servidor DNS)

etc.

A continuación se muestran una serie de capturas acerca de su funcionamiento:

EJEMPLO 1 - Reconociendo un servidor DNS con BIND 8 que no proporciona información alguna:

- En sistemas unix:

```
[root@VaxMAN]host -t ns google.com (para buscar los servidores
DNS de google)
google.com name server ns4.google.com
google.com name server ns1.google.com
google.com name server ns2.google.com
google.com name server ns3.google.com
```

```
[root@VaxMAN]host -t txt version.bind ns1.google.com.
Using domain server:
Name: ns1.google.com
Address: 216.239.32.10#53
Aliases:
Host version.bind not found: 5(REFUSED) (no se obtiene
información acerca del software o la versión)
```

- En sistemas windows:

```
D:\VaxMAN>nslookup
Servidor predeterminado: dns.terra.es
Address: 195.235.113.3
>set class=chaos
>set querytype=txt
>version.bind ns1.google.com.
Servidor: ns1.google.com
Address: 216.239.32.10
*** No hay registros text (TXT) disponibles para version.bind
```

- Utilizando `fpdns.pl`

```
[root@VaxMAN fpdns]perl fpdns.pl ns1.google.com
fingerprint (ns1.google.com, 216.239.32.10): BIND 8.3.0-RC1 --
8.4.4 (con fpdns se obtiene el software y la versión del
software instalado en el servidor DNS)
```

EJEMPLO 2 - Reconociendo un servidor DNS con BIND 9 que tiene la versión del software ofuscada:

- En sistemas unix:

```
[root@VaxMAN]host -t ns terra.com (para buscar los servidores
DNS de terra)
terra.com name server ns1.terra.com
terra.com name server ns2.terra.com
[root@VaxMAN]host -c chaos -t txt version.bind ns2.terra.com.
Using domain server:
Name: ns2.terra.com
Address: 66.119.66.63#53
Aliases:
version.bind text "surely you must be joking" (banner o texto
introducido en el named.conf para ofuscar la versión del
software y el programa DNS utilizado)
```

- En sistemas Windows:

```
D:\VaxMAN>nslookup
Servidor predeterminado: dns.terra.es
Address: 195.235.113.3
> set class=chaos
> set querytype=txt
> version.bind ns2.terra.com.
Servidor: ns2.terra.com
Address: 66.119.66.63
version.bind text =
"surely you must be joking" (banner o texto introducido en el
named.conf para ofuscar la versión del software y el programa
DNS utilizado)
```

- Con fpdns.pl

```
[root@VaxMAN fpdns]perl fpdns.pl ns2.terra.com
fingerprint (ns2.terra.com, 66.119.66.63): BIND 9.2.3rc1 --
9.4.0a0 (con fpdns se obtiene el software y la versión del
software instalado en el servidor DNS)
```

EJEMPLO 3 - Reconociendo un Servidor DNS MS Windows 2003

```
[root@VaxMAN]host -t ns microsoft.com (para buscar los
servidores DNS de microsoft)
microsoft.com name server ns1.msft.net
microsoft.com name server ns2.msft.net
microsoft.com name server ns3.msft.net
```

```
microsoft.com name server ns4.msft.net
microsoft.com name server ns5.msft.net
```

- Desde sistemas unix:

```
[root@VaxMAN]host -c chaos -t txt version.bind ns1.msft.net.
Using domain server:
Name: ns1.msft.net
Address: 207.46.245.230#53
Aliases:
Host version.bind not found: 4(NOTIMP) (no se obtiene
información acerca del software o la versión)
```

- Desde sistemas Windows:

```
D:\VaxMAN>nslookup
Servidor predeterminado: dns.terra.es
Address: 195.235.113.3
> set class=chaos
> set querytype=txt
> version.bind ns1.msft.net.
Servidor: ns1.msft.net.
Address: 207.46.245.230
DNS request time out.
timeout was 2 seconds
*** ns1.msft.net. no se puede encontrar version.bind: Not
implemented (como no se está utilizando el software BIND no se
puede facilitar la versión)
```

- Con fpdns.pl

```
[root@VaxMAN fpdns]perl fpdns.pl ns1.msft.net
fingerprint (ns1.msft.net, 207.46.245.230): Microsoft Windows
2003 (con fpdns se obtiene el software y la versión del
software instalado en el servidor DNS)
```

EJEMPLO 4 - Aumentando el timeout a 5 para reconocer el servidor DNS

En determinados escenarios, cuando la carga del servidor DNS es elevada, podemos aumentar el tiempo de espera empleando para ello el parámetro `-t`, este tiempo especificado en segundos evitará que las peticiones caduquen antes de obtener la versión del software de DNS.

```
[root@VaxMAN]host -t ns linkara.com (para buscar los
servidores DNS de linkara)
linkara.com name server ns1.eu.dedicatedserver.com
linkara.com name server ns0.eu.dedicatedserver.com
```

```
[root@VaxMAN]host -c chaos -t txt version.bind
ns1.eu.dedicatedserver.com.
Using domain server:
Name: ns1.eu.dedicatedserver.com.
Address: 213.198.65.226#53
Aliases:
Host version.bind not found: 1(FORMERR)
```

▪ Desde sistemas Windows:

```
D:\VaxMAN>nslookup
Servidor predeterminado: dns.terra.es
Address: 195.235.113.3
> set class=chaos
> set querytype=txt
> version.bind ns1.eu.dedicatedserver.com.
Servidor: ns1.eu.dedicatedserver.com.
Address: 213.198.65.226
*** ns1.eu.dedicatedserver.com. no se puede encontrar
version.bind: Format error (no se obtiene información acerca
de la versión y el software DNS)
```

▪ Con fpdns.pl

```
[root@VaxMAN fpdns]perl fpdns.pl ns1.eu.dedicatedserver.com.
fingerprint (ns1.eu.dedicatedserver.com., 213.198.65.226):
q0r8qlr?query timed out (no se obtiene información por un
timeout)
```

```
[root@VaxMAN fpdns]perl fpdns.pl -t 5
ns1.eu.dedicatedserver.com.
fingerprint (ns1.eu.dedicatedserver.com., 213.198.65.226):
TinyDNS 1.05 (aumentando el timeout se consigue obtener la
versión y el programa DNS utilizado)
```

Source URL:

<http://www.hacktimes.com/?q=node/28>

Links:

[1] <http://www.securityfocus.com>

[2] <http://www.rfc.se/fpdns/>

[3] <http://www.net-dns.org>