PaperLab

Hacking Ético

Seguridad Informática

"El buscador"

Revisión 2 - 10.11

José luis Prado Seoane

En este laboratorio práctico simulado se le explicará como un atacante va recopilando todo tipo de información que le permitirá ir conformando un "mapa" técnico de lo que tiene entre manos, - *que servicios hay, tipos, grados de exposición, linkeados a Bases de Datos - si se diera el caso -, tecnologías, y un sin fin de datos como hemos comentado anteriormente* -, para posteriormente, - *y tal como veremos en los próximos capítulos* - , empezar a entender más .. , determinar vectores, documentarse y empezar a planificar la estrategia de compromiso del sistema o Infraestructura. En una correcta planificación del mismo radicará su éxito y ahí radica la verdadera importancia de la recopilación de información, ¡ saber es poder!, y recuerde, no subestime nunca cualquier posible información con exposición pública.

Se intentará transmitir de una forma técnica y ordenada el procedimiento, por lo que animamos al lector a que experimente con diferentes situaciones derivadas que le permita consolidar los conceptos que en él se transmitirán. Ya sabe, si conoce a su enemigo, sabrá más de él y aprenderá a protegerse con eficacia.

Dominio público ficticio: centraltermica.xxx
Dominio Local o privado: centraltermica.lan

Con independencia de la recopilación de otra información asociada, un atacante empezará a mirar qué hay detrás del dominio (centraltermica.com), es lo lógico, y será un buen punto de partida para entender los conceptos, por lo que buscará..; IP´s asociadas, registros, servidores Whois, servidores de nombres DNS - *preste atención a estos parámetros* -, estado actual, fechas Update, fechas de creación y expiración, nombre del contacto administrativo - *nunca se sabe, lo podría utilizar para un ataque de Ingeniería Social* -, su e-mail asociado, teléfonos, Referral URL - *preste atención a este parámetro* -, etc.-.

Antes de nada deberá instalar el programa Whois en su terminal de trabajo en función de la Distro de que disponga, en el caso de Backtrack que es la que estamos utilizando para estos Labs ejecute el siguiente comando:

```
root@lab:/# apt-get install whois
```

A continuación pregunte sobre el dominio especificado con la aplicación "Whois" para que le devuelva la información de los registros correspondientes. Debe tener en cuenta que el propietario del dominio puede tener limitado el Reply de los mismos para proporcionar una limitación de información a terceros por seguridad, así mismo, todo está en función del proveedor de servicios de Hosting en el caso de una externalización, en algunos casos protegerá los mismos por petición y pago del propietario, y otros no tendrán implementado esta opción sin más. En el caso de una entidad con su propia infraestructura esta tarea corresponderá al administrador del sistema, ya se sabe, cuanto menos información se exponga mejor.

```
root@lab:/# whois centraltermica.xxx
```

(Se especifican los datos más relevantes)

```
Whois Server Version X.X
```

…
Server Name: centraltermica.xxx
IP Address: 2XX.XXX.XXX.32
Registrar: INFRAESTRUCTURAS CRITICAS, S.L.
Whois Server: whois.infraestructurascriticas22.xxx
Referral URL: http://www. centraltermica.xxx
Domain Name: centraltermica.xxx
…
Name Server: NS1. centraltermica.xxx
Name Server: NS2. centraltermica.xxx
…
Expiration Date: 29-Mar-2007
Registrant:
XX XXXXXXX St.
Madrid xxxxx
SPAIN
Administrative Contact, Technical Contact:
Carlos XXX carlosxxx@ centraltermica.xxx
…
Domain servers in listed order:
NS1. centraltermica.xxx 1XX.XX.XX.180
NS2. centraltermica.xxx 2XX.XXX.XXX.24

(*) Ejemplo ficticio y simulado a 11/04/2014

En la salida devuelta por la aplicación podemos observar algunos registros de información general pero igual de valiosos, y otros de vital importancia para un atacante como, Referral URL, dónde podemos ver especificado que dicho dominio expone un servicio HTTP Web hacia una máquina física o virtual y su IP asociada (IP Address).

Para un atacante la información de principal interés son los servidores de nombres (NS) que como hemos comentado anteriormente pueden a petición, devolver un COPY de lo que hay detrás (transferencia de zona), y encaminar al mismo hacia la red o redes de la entidad (Intranet), asociado todo ello, principalmente a una mala configuración del administrador del sistema. Intentará encontrar además otros servicios asociados al dominio, que con la información que tiene en su poder obtenida por diferentes fuentes o técnicas sumado a su experiencia, conocimiento, etc.- , puede intuir, y por consiguiente, empezará a "jugar" con la red pública, - *ahí entran en juego todo tipo de sistemas de seguridad perimetral que estudiaremos más adelante* -.

(**Practica 1**: Juegue un poco con su buscador preferido en búsqueda de servicios asociados a su dominio y comprenderá mejor lo que se le expone)

Un atacante siempre intentará alcanzar el mayor botín, - *con independencia de la finalidad de la intrusión* -, siempre a través del eslabón más débil o menos protegido además, entendiendo que por costes o eficiencia en el funcionamiento ninguna entidad asumirá el coste que supondría proteger su infraestructura o sistema al cien por cien, - *es algo que no tiene lógica y no es viable* -, siempre se protegerá, lo que más valor tiene para su continuidad y negocio.

Como ha podido observar en la salida de la anterior petición Whois hemos obtenido dos registros que exponen un servicio público Web (Referral URL / IP) , pregunte nuevamente, pero esta vez estableciendo como parámetro la IP obtenida asociada.

root@lab:/# proxychains whois 2XX.XXX.XXX.32
…

Information related to 2XX.XXX.210.20 - 2XX.XXX.210.50'
…

Como puede observar la información devuelta nos muestra un rango de IP´s pero aún así, se deberá tener en cuenta que existe la posibilidad , - *lo más seguro* -, y principalmente si se trata una externalización del servicio, un filtrado por parte del proveedor además, dicha solicitud le devolverá otros parámetros que deberá contrastar con la anterior solicitud. Una vez determinados los registros principales, analizados en búsqueda de servicios públicos, rangos de máquinas, etc.-, comenzaremos con el análisis de los DNS para intentar extraer la máxima información disponible.

Para ello utilizaremos la herramienta de trabajo Nslookup y estableceremos un servidor local Bind en una configuración básica que le permita realizar la práctica en un entorno real. Recuerde que hay dos tipos de servidores, los usados en Internet que son públicos y entrelazados, que traducen los nombres de dominios, y los internos a un red local, como en el ejemplo que definiremos a continuación, que resuelven nombres de host a sus

correspondientes IP´s privadas, no aceptando peticiones externas pero sí, pueden ser configurados para conectarse a los DNS asignados por el proveedor de Internet en la búsqueda de resolución de nombres de dominio. La versión que instalaremos es la (9).

root@lab:/# apt-get install bind9 dnsutils (instalamos el servidor)

Diríjase al directorio de configuración "/etc/bind" y edite en primer lugar el archivo " named.conf " con el editor "nano", - podrá usar el editor grafico que desee pero le aconsejo que se familiarice con los editores de consola "vi", "nano" u otros similares -. La documentación para la configuración de este archivo podrá encontrarla públicamente en Internet o simplemente, instalando su "bind9-doc" a través nuevamente de APT. Empecemos ..

root@lab:/# cd /etc/bind

root@lab:/etc/bind# nano named.conf

Establezca únicamente estas líneas "include" que ya vienen por defecto.

```
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
nclude "/etc/bind/named.conf.default-zones";
```

Edite el archivo "named.conf.options" dónde estableceremos las IP´s de los DNS suministrados por su ISP para resolver dominios públicos. (Advertencia: mantenga las mismas tabulaciones, puntos y comas, etc.-, que el ejemplo, para todos los archivos de configuración que se mostrarán a continuación)

root@lab:/etc/bind# nano named.conf.options

```
options {
  directory "/var/cache/bind";
forwarders {
  80.xx.xx.xxx;
  80.xx.xx.xxx;
};
  auth-nxdomain no;
  listen-on-v6 { any; };
};
```

Edite el archivo "named.conf.local" dónde establecerá los archivos del maestro y el de su resolución inversa para el dominio de ejemplo.

root@lab:/etc/bind# nano named.conf.local

```
zone " centraltermica.lan" {
  type master;
  file "/etc/bind/2ghoww45.db";
};
zone "1.168.192.in-addr.arpa" {
  type master;
  file "/etc/bind/192.rev";
};
```

Cree y edite el archivo "2ghoww45.db" dónde establecerá los nombres de los Hosts e IP´s correspondientes.

root@lab:/etc/bind# nano 2ghoww45.db

```
;
; BIND centraltermica.lan
;
@ IN SOA centraltermica.lan. root.centraltermica.lan. (
                1 ; Serial
                604800 ; Refresh
                86400 ; Retry
                2419200 ; Expire
                604800 ) ; Default TTL
                IN NS ns1.centraltermica.lan.
                IN MX 5 mail1.centraltermica.lan.
                IN MX 10 mail2.centraltermica.lan.
                IN MX 20 mail3.centraltermica.lan.
ns1 IN A 192.168.1.37 ← (Establezca aquí la IP asignada a su tarjeta de red)
ftp IN A 192.168.1.100
```

```
administracion IN A 192.168.1.101
contabilidad IN A 192.168.1.102
facturacion IN A 192.168.1.103
backup IN A 192.168.1.104
fichastecnicas IN A 192.168.1.105
mail1 IN A 192.168.1.106
mail2 IN A 192.168.1.107
mail3 IN A 192.168.1.108
login IN A 192.168.1.109
router IN A 192.168.1.200
www IN A 192.168.1.250
```

Cree y edite el archivo "192.rev" para establecer la resolución inversa.

```
root@lab:/etc/bind# nano 192.rev

;
; BIND reverse centraltermica.lan
;
@ IN SOA centraltermica.lan. root.centraltermica.lan. (
                                        1 ; Serial
                                        604800 ; Refresh
                                        86400 ; Retry
                                        2419200 ; Expire
                                        604800 ) ; Default TTL
                                        IN NS ns1.centraltermica.lan.
37 IN PTR ns1.centraltermica.lan.
100 IN PTR ftp.centraltermica.lan.
101 IN PTR administracion.centraltermica.lan.
102 IN PTR contabilidad.centraltermica.lan.
103 IN PTR facturacion.centraltermica.lan.
104 IN PTR backup.centraltermica.lan.
105 IN PTR fichastecnicas.centraltermica.lan.
106 IN PTR mail1.centraltermica.lan.
107 IN PTR mail2.centraltermica.lan.
108 IN PTR mail3.centraltermica.lan.
109 IN PTR login.centraltermica.lan.
200 IN PTR router.centraltermica.lan.
250 IN PTR www.centraltermica.lan.
```

Una vez configurado y creado los archivos correspondientes deberá indicarle a su máquina que es el servidor DNS, modificando el archivo de configuración "resolv.conf" en el directorio "/etc" tal y como se indica a continuación.

```
root@lab:/# cd /etc
root@lab:/etc# nano resolv.conf

nameserver 127.0.0.1
search centraltermica.lan
```

No olvide que deberá hacer lo mismo en los diferentes Hots de su ámbito de red pero esta vez indicando la IP correspondiente "nameserver 192.168.1.37" (Eth) o configurando el DNS local en función del tipo de Sistema Operativo.

(**Practica 2**: Establezca el arranque automático del servidor Bind en su máquina estableciendo en enlace simbólico correspondiente a uno o varios de los diferentes niveles (rc´s) de arranque del sistema)

Arrancamos el servidor DNS, y recordemos que tenemos un servidor DNS "NS=ns1" asociado al dominio local "centraltermica.lan" que resuelve o "agrupa" un conjunto de máquinas físicas o virtuales entre las que se encuentra un servidor Web (www), tres servidores de correo (mail), entre otros.

```
root@lab:/# /etc/init.d/bind9 start
```

Parar: `root@lab:/# /etc/init.d/bind9 stop`
Reiniciar: `root@lab:/# /etc/init.d/bind9 restart`

Una vez montado y finalizado la configuración de nuestro servidor y haber comprobado que resuelve peticiones "host", (root@lab:/# host 192.168.1.37, root@lab:/# host ns1.centraltermica.lan, host www.google.es, etc..),

empecemos a determinar que hay detrás del mismo tal y como un atacante actuaria. Para ello utilizaremos como hemos comentado la herramienta “Nslookup”.

```
nslookup [-option] [name | -] [server]
```

(**Practica 3**: Ejecute el comando “man nslookup”, analice su contenido y experimente).

Empecemos intentando una resolución básica a una de las máquinas asociadas al dominio, en nuestro caso (www), desde otra máquina cualquiera de nuestra Red, - recuerde que deberá establecer la IP que apunte al mismo -.

```
root@lab:/# nslookup

> www.centraltermica.lan

Server: 192.168.1.37
Address:        192.168.1.37#53

Name:   www.centraltermica.lan
Address: 192.168.1.250
```

Como podrá observar nos muestra la IP asociada (address) al servidor DNS que suministra resoluciones asociadas al dominio “centraltermica.lan”, - *el camino a seguir para el acceso a la información* -, además, nos devuelve la resolución (IP) de la máquina asociada (www).

Empecemos a examinar un poco buscando posibles servidores de nombres(NS) que permitan ampliar la información.

```
> set type=ns
> centraltermica.lan      (Preguntamos al dominio)

Server: 192.168.1.37
Address:        192.168.1.37#53

centraltermica.lan nameserver = ns1.centraltermica.lan.
```

Como ha podido observar nos devuelve el único servidor DNS (ns) existente, como es lógico, tal y como lo hemos establecido en nuestra configuración. Debe tener en cuenta que los servidores DNS pueden ser zonales, es decir, encontrarse en diferentes departamentos o edificios dentro de la red interna de la empresa u entidad, y de igual forma, en todos aquellos de carácter público, tenga esto siempre en cuenta.

(**Practica 4**: Monte otro servidor DNS en una máquina virtual, asócielo a este mismo dominio, configúrelos y vuelva a realizar la consulta)

Una de las tareas rutinarias que deberá realizar periódicamente a través de esta y otras herramientas similares en su sistema, es determinar la visibilidad de sus servidores DNS locales, y su respuesta o no a una petición de resolución pública. Imagínese que preguntamos a nuestro servidor DNS Local interno (ns1.centraltermica.lan) y además, necesitara comprobar que una posible consulta sobre un servidor DNS externo cualquiera, - *elija el que quiera* -, no debería encontrar su dirección.

Empezaremos estableciendo el server local (> server) que en este caso es nuestro servidor DNS como hemos señalado, y posteriormente realizaremos una consulta pública y veremos lo que sucede.

```
root@lab:/# nslookup

> server 192.168.1.37

Default server: 192.168.1.37
Address:        192.168.1.37#53

> ns1.centraltermica.lan          (Aquí realizamos o preguntamos al server)

Server: 192.168.1.37
Address:        192.168.1.37#53

Name: ns1. centraltermica.lan
Address: 192.168.1.37
```

Como ha podido observar, ha sido todo correcto hasta el momento. A continuación realizaremos una consulta en un servidor DNS externo cualquiera, - *DNS´s de nuestro ISP por ejemplo* - hacia un IP pública conocida, - *un portal Web que conozca su IP* -, el cuál, le debería resolver sin ningún problema el nombre de su máquina asociada. Finalizaremos realizando la consulta de una de nuestras máquinas internas a través de ese DNS externo, el cuál, no nos debería resolver, como es lógico, ya que este no debería estar expuesto al exterior.

Imagínese por un solo momento las consecuencias de una exposición pública no controlada derivada de un fallo de configuración de una máquina del dominio interno como por ejemplo, "login.centraltermica.lan", la cuál establece una acceso interno de Login para la consulta técnica de documentos de configuración , topologías, dispositivos, etc.-, montado en PHP sin parchear desde hace un par de años, por no decir más, del personal técnico de la empresa u organización, estaríamos ante un grave problema de seguridad.

```
root@lab:/# nslookup

> server 80.xx.xx.xxx        (DNS externo cualquiera)
Default server: 80.xx.xx.xxx
Address: 80.xx.xx.xxx#53
> 193.xxx.12x.xx9          (Preguntamos por una IP pública conocida cualquiera)
Server:    80.xx.xx.xxx
Address:        80.xx.xx.xxx#53

Non-authoritative answer:
193.xxx.12x.xx9.in-addr.arpa    name = www3.xxxxxxxxxx.es.  (Responde)

> login.centraltermica.lan   (Preguntamos por la máquina interna de nuestro dominio interno)

Server: 80.xx.xx.xxx
Address:        80.xx.xx.xxx#53

** server can´t find login.centraltermica.lan: NXDOMAIN
```

La configuración de nuestro DNS interno al exterior es correcta y no se expone al exterior. No olvide está sencilla técnica de comprobación que le puede ahorrar problemas a la hora de mantener segura la Infraestructura que tenga a su cargo. Tras esta comprobación básica y necesaria continuamos buscando los servidores de correo (mx) que hemos configurado para nuestro servidor DNS.

```
> server 192.168.1.37

Default server: 192.168.1.37
Address: 192.168.1.37#53

> set type=mx
> centraltermica.lan        (Preguntamos al dominio)

Server: 192.168.1.37
Address:        192.168.1.37#53

centraltermica.lan      mail exchanger = 5 mail1.centraltermica.lan.
centraltermica.lan      mail exchanger = 10 mail2.centraltermica.lan.
centraltermica.lan      mail exchanger = 20 mail3.centraltermica.lan.
```

La salida nos devuelve lo esperado, tres servidores de correo (mail servers) con un índice numérico que simplemente le indicará en un entorno real, la prioridad en la recepción de los mensajes de unos sobre otros, la misma será de menor a mayor, cuanto más pequeño sea el valor numérico más prioritario será.

En este ejemplo, el servidor de correo (5) (mail1.centraltermica.lan.) será el principal o primario y el resto atendiendo a su valor numérico, Relays del mismo.

No olvide que con la práctica se adquiere la destreza y experiencia suficiente para poder "bucear" a través de la cantidad de datos que se van obteniendo con las diferentes herramientas disponibles además, todo atacante avanzado dispondrá de sus propios trucos, técnicas y Scripts que le permitirán "automatizar" y agilizar, - *como verá a continuación* -, este proceso de búsqueda y análisis, el límite lo podrá su perseverancia y conocimiento.

Intentará determinar en primer lugar por "fuerza bruta" las máquinas (nombres) asociadas al dominio, y ¿Como lo hará?, básicamente utilizando la información recopilada o intuyendo posibles nombres existentes, intentando resolver y registrar los mismos. La idea o la técnica es muy sencilla, pero a la vez muy eficaz, y le permitirá

poder “automatizar” el proceso, - *y no lo olvide* -, sus presas son esas IP´s y nombres que le acerquen a su objetivo, el compromiso.

Para entender mejor el proceso utilizaremos la sencilla herramienta de trabajo “host”, utilizada como hemos visto en alguno de los párrafos anteriores para realizar búsquedas DNS, y nos permitirá convertir nombres a direcciones IP y viceversa.

host [-aCdlnrsTwv][-c class][-N ndots][-R number][-t type][-W wait][-m flag][-4][-6] {name}[server]

(**Practica 5**: Ejecute el comando “man host”, analice su contenido y experimente)

Al ejecutar “host” con un nombre inexistente contra un dominio ejemplo.-, (vpn345ft2.centraltermica.lan), no podrá resolverse, y nos devolverá el “not found” correspondiente. Un atacante tiene dos opciones, la primera es ir probando uno a uno de forma manual “nombre.dominio”, - *algo del todo poco recomendable*-, y la segunda la aconsejable, la generación de un Script que le ayudara en su tarea. Para ello utilizaremos el lenguaje Python por su versatilidad, rapidez y sencillez aunque puede utilizar cualquier otro, es indiferente, y no olvide que cuanto más lenguajes conozca mayor capacidad técnica tendrá, por lo que a lo largo del libro utilizaremos otros lenguajes de programación principalmente ANSI-C o Perl, entre otros.

En primer lugar crearemos nuestra pequeña Base de Datos en modo texto en un archivo en disco con todos los nombres que intentemos resolver, el mismo será dinámico y lo podrá utilizar para otras ocasiones en sus pruebas de seguridad. Si lo prefiere podría buscar diccionarios en Internet relacionados, pero tenga cuidado con lo que descarga y más este tipo de contenidos que suelen estar infectados por Malware.

root@lab:/# nano nombreserv.txt (Creamos la Base de datos o diccionario)*

ns1
ns2
ns3
ns4
www
www2
ftp
smtp
mail
mail1
mail2
mail3
mail4
exchange
pop3
proxy
vpn

firewall
router
gateway
comercial
comerciales
fichas
login
fichastecnicas
jefe
administracion
contabilidad
facturacion
remoto
backup
fire
virtual
. . .

ns1 **(*)**
ns2
ns3
ns4
www
www2
ftp
smtp
mail
mail1
mail2
mail3
mail4
exchange
pop3
proxy
vpn
firewall
router
gateway
comercial
comerciales
fichas
login
fichastecnicas
jefe
administracion
contabilidad
facturacion
remoto
backup
fire
virtual
. . .

(*) archivo en modo texto continuo.

A continuación desarrollaremos un sencillo Script al que denominaremos “resolverdb.py” que utilizará la base de datos creada para comprobar uno a uno, - *determinación por “Fuerza Bruta”* - , la existencia de los mismos contra un dominio que especificaremos, en nuestro caso “centraltermica.lan”, en la búsqueda y almacenamiento de relaciones de Hosts existentes y su Ip, (Host:Ip). Cree con Nano un archivo denominado “filtradodirecto.txt” que recoja la información sintetizada en disco. No olvide que está realizando esta técnica contra un dominio local (centraltermica.lan), pero ante un caso real, - *un dominio público* -, que expone algunas máquinas públicas abiertamente como las (www.) y otras no (principalmente aquellas que puedan indicar otras redes internas), un atacante intentará complementar la técnica anterior con un análisis de los DNS asociados al dominio, - *como veremos en los próximos párrafos* -, que le informen de todas las máquinas e IP´s existentes, y todo ello por supuesto, “ocultándose” en la red.

resolverdb.py

```
#!/usr/bin/env python
# -*- coding: latin-1 -*-

#Versión:Python 2.7.6
```

```
#Check 07/04/2014
#Sistema:Backtrack5_release_10.04
#Kernel:linux 2.6.38
#Puede copiar,modificar y publicar este codigo en el medio que desee
#haciendo referencia de origen al autor del mismo.
#Utilice el mismo con responsabilidad en entornos seguros y controlables

import os,sys,commands

origen = open('nombreserv.txt','r')
filtrado = open('filtradodirecto.txt','r+')
dominio = raw_input("Dominio de análisis: ")
maquinas = origen.readlines()
print ""
print ("Dominio: %s" %(dominio))
print ""

for host in maquinas[:-1]:

    resolucion = os.system ("host %s.%s > /dev/null" % (host[0:-1],dominio))

    if ( resolucion == 0 ) :
            resultado = commands.getoutput("host %s.%s" % (host[0:-1],dominio))
       filtrado.write(resultado.replace("%s.%s has address " % (host[0:-1],dominio),"") + "\n")
            print resultado.replace("%s.%s has address " % (host[0:-1],dominio),"")

print ""
origen.close()
filtrado.close()
```

Una vez creado y editado el archivo “resolverdb.py”, hágalo ejecutable (compruébelo con el comando “ls –l”) y ejecútelo especificando el dominio local para proceder al análisis por Fuerza Bruta..

```
root@lab:/# chmod +x resolverdb.py

root@lab:/# python resolverdb.py

Dominio de análisis: centraltermica.lan

Máquinas: Host/Ip ----------

ns1 : 192.168.1.37
www : 192.168.1.250
mail1 : 192.168.1.106
mail2 : 192.168.1.107
mail3 : 192.168.1.108
ftp : 192.168.1.100
login : 192.168.1.109
router : 192.168.1.200
fichastecnicas : 192.168.1.105
administracion : 192.168.1.101
contabilidad : 192.168.1.102
facturacion : 192.168.1.103
backup : 192.168.1.104
```

Con un trabajo de Ingeniería Social amplio y bien definido, un atacante podría crear un diccionario más potente y convertir esta sencilla técnica en un arma de recopilación directa de IP´s y otras posibles redes o subredes relacionadas con el dominio muy poderosa. Imagínese que en la información obtenida con anterioridad se hubiera determinado por ejemplo.-, “gateway : 172.16.0.1”, estaríamos ante otro camino o vía a seguir si analizáramos el posible rango asociado.

Desarrollaremos a continuación otra vía de análisis en la búsqueda de IP’s ocultas que a su vez, es complementaria con lo desarrollado con anterioridad, que implementaremos modificando el anterior Script guardándolo en disco como “resolverdb2.py”, que le permitirá acercarse a la topología real de la Infraestructura. Basada en la resolución inversa, analiza la posibilidad de obtener máquinas ocultas no directas y diferentes redes, por lo que en nuestro caso, será sencillo, ya que nos encontramos ante una única red de clase C “192.168.1. 0/24” en la que automatizaremos el proceso para entender el concepto.

(**Practica 6-recomendable-)**: Adapte el servidor Bind local para crear otras redes simuladas e implemente cambios en el Script para automatizar un árbol de búsqueda lineal que analice y determine las diferentes redes obtenidas por la resolución directa, optimice la herramienta, establezca controles de depuración, codifique

tratamiento de nodo (diferentes máquinas asociadas a una misma IP), y si se encuentra con ánimo, podría adornarlo un poco, aunque ya sabe , no es su finalidad. En la actualidad esta herramienta avanzada de análisis para el Research para mi uso personal, implementa más de cuarenta procesos paramétricos de captación de información, por lo que le animo a que evolucione esta base de codificación de acuerdo a sus necesidades de Seguridad. Recuerde:

Red 255	Host 0	Host0	Host0	**Clase A/8**
Red 255	**Red 255**	Host 0	Host 0	**Clase B/16**
Red 255	**Red 255**	**Red 255**	Host 0	**Clase C/24**

Comencemos creando con Nano en la misma ruta en disco un archivo denominado "filtradoinverso.txt" que recoja la salida de la herramienta además, modificaremos nuestro Bind inverso (192.rev) añadiendo más hosts asociados a la Red. Siempre que le sea posible, - y si utiliza Linux en su trabajo ordinario, algo que le aconsejo -, distribuya la información de salida de las herramientas en diferentes archivos que le permita procesarla y "pipearla" con mayor rapidez y sencillez.

```
root@lab:/etc/bind# nano 192.rev

;
; BIND reverse centraltermica.lan
;
@ IN SOA centraltermica.lan. root.centraltermica.lan. (
                                        1 ; Serial
                                        604800 ; Refresh
                                        86400 ; Retry
                                        2419200 ; Expire
                                        604800 ) ; Default TTL
                                        IN NS ns1.centraltermica.lan.
37 IN PTR ns1.centraltermica.lan.
100 IN PTR ftp.centraltermica.lan.
101 IN PTR administracion.centraltermica.lan.
102 IN PTR contabilidad.centraltermica.lan.
103 IN PTR facturacion.centraltermica.lan.
104 IN PTR backup.centraltermica.lan.
105 IN PTR fichastecnicas.centraltermica.lan.
106 IN PTR mail1.centraltermica.lan.

. . .

233 IN PTR luces.centraltermica.lan.
234 IN PTR alarmas.centraltermica.lan.
235 IN PTR perimetros.centraltermica.lan.
236 IN PTR personal.centraltermica.lan.
237 IN PTR motores.centraltermica.lan.
238 IN PTR central.centraltermica.lan.
239 IN PTR mandoycontrol.centraltermica.lan.
240 IN PTR comunicaciones.centraltermica.lan.
241 IN PTR micros.centraltermica.lan.
242 IN PTR partnumbers.centraltermica.lan.
243 IN PTR imagen1.centraltermica.lan.
244 IN PTR imagen2.centraltermica.lan.
245 IN PTR backupconfig.centraltermica.lan.
246 IN PTR resets.centraltermica.lan.
247 IN PTR remoto2.centraltermica.lan.
250 IN PTR www.centraltermica.lan.
```

resolverdb2.py

```
#!/usr/bin/env python
# -*- coding: latin-1 -*-

#Versión:Python 2.7.6
#Check 07/04/2014
#Sistema:Backtrack5_release_10.04
```

```
#Kernel:linux 2.6.38
#Puede copiar,modificar y publicar este codigo en el medio que desee
#haciendo referencia de origen al autor del mismo.
#Utilice el mismo con responsabilidad en entornos seguros y controlables

import os,sys,commands

origen = open('nombreserv.txt','r')
filtradodirecto = open('filtradodirecto.txt','w+')
filtradoinverso = open('filtradoinverso.txt','w+')
dominio = raw_input("Dominio de análisis: ")
maquinas = origen.readlines()
print ""
print ("Análisis por diccionario..: %s" %(dominio))
print ""

for host in maquinas[:-1]:

  resolucion = os.system ("host %s.%s > /dev/null" % (host[0:-1],dominio))

  if ( resolucion == 0 ) :
        resultado = commands.getoutput("host %s.%s" % (host[0:-1],dominio))
     filtradodirecto.write(resultado.replace("%s.%s has address " % (host[0:-1],dominio),"") + "\n")
        print resultado.replace("%s.%s has address " % (host[0:-1],dominio),"")

print ""
print ("Análisis inverso de Hosts ocultos en la Red..")
print ""

for equipo in range(255):

  resolucioninversa = os.system ("host 192.168.1.%s > /dev/null" % (equipo))

  if ( resolucioninversa == 0 ) :
        resultadoinverso = commands.getoutput("host 192.168.1.%s" % (equipo))
        inicial = resultadoinverso.find("pointer")
     filtradoinverso.write("192.168.1.%s : %s" % (equipo,resultadoinverso[(inicial + 8):-1]) + "\n")
        print ("192.168.1.%s : %s" % (equipo,resultadoinverso[(inicial + 8):-1]))

print ""
origen.close()
filtradodirecto.close()
filtradoinverso.close()
```

Una vez creado y editado el archivo “resolverdb2.py”, reinicie el servidor DNS y ejecute la herramienta especificando el dominio local ..

```
root@lab:/# /etc/init.d/bind9 restart

root@lab:/# python resolverdb2.py
Dominio de análisis: centraltermica.lan

Análisis por diccionario..: centraltermica.lan

192.168.1.34
192.168.1.250
192.168.1.106
192.168.1.107
192.168.1.108
192.168.1.100
192.168.1.109
192.168.1.200
192.168.1.105
192.168.1.101
192.168.1.102
192.168.1.103
192.168.1.104

Análisis inverso de Hosts ocultos en la Red..

192.168.1.34 : ns1.centraltermica.lan
192.168.1.100 : ftp.centraltermica.lan
192.168.1.101 : administracion.centraltermica.lan
192.168.1.102 : contabilidad.centraltermica.lan
```

192.168.1.103 : facturacion.centraltermica.lan
192.168.1.104 : backup.centraltermica.lan
192.168.1.105 : fichastecnicas.centraltermica.lan
192.168.1.106 : mail1.centraltermica.lan
192.168.1.107 : mail2.centraltermica.lan
192.168.1.108 : mail3.centraltermica.lan
192.168.1.109 : login.centraltermica.lan
192.168.1.200 : router.centraltermica.lan
192.168.1.220 : contactores.centraltermica.lan
192.168.1.221 : valvulas.centraltermica.lan

. . .

192.168.1.234 : alarmas.centraltermica.lan
192.168.1.235 : perimetros.centraltermica.lan
192.168.1.236 : personal.centraltermica.lan
192.168.1.237 : motores.centraltermica.lan
192.168.1.238 : central.centraltermica.lan
192.168.1.239 : mandoycontrol.centraltermica.lan
192.168.1.240 : comunicaciones.centraltermica.lan
192.168.1.241 : micros.centraltermica.lan
192.168.1.242 : partnumbers.centraltermica.lan
192.168.1.243 : imagen1.centraltermica.lan
192.168.1.244 : imagen2.centraltermica.lan
192.168.1.245 : backupconfig.centraltermica.lan
192.168.1.246 : resets.centraltermica.lan
192.168.1.247 : remoto2.centraltermica.lan
192.168.1.250 : www.centraltermica.lan

Finalizaremos este laboratorio analizando otra de las numerosísimas vías de búsqueda de información utilizada por los atacantes en la actualidad, - *las transferencias de zona, es decir lo que hay detrás*.. . Para ello se analizan los servidores de nombres (NS) existentes, que en nuestro caso es único "ns1.centraltermica.lan".

Un mal atacante interno, - *pero no menos peligroso* -, a la red, podría no complicarse tanto la vida y para ello terminaría montando un esclavo en algún host del segmento que apunte a su objetivo (server), para terminar realizando un COPY después de hacerle al servidor una denegación de servicio en toda regla, que lo reiniciase automáticamente en función de los procesos de activación de servicios (daemons) o del propio administrador del sistema eso si, saltando todas las alarmas habidas o por haber.

En primer lugar cree un archivo en disco denominado "filtradozonas.txt" que recoja la información de la herramienta a la que denominaremos "resolverdb3.py" basado en la modificación del Script anterior. No olvide que deberá garantizar la seguridad de su servidor DNS de terceros sin autorización para ello, se aconseja instalar dichos servidores detrás de un cortafuegos debidamente configurado para tal efecto, que el mismo sea dedicado, por supuesto no lo ejecute nunca como root, evite cualquier consulta DNS no autorizada creando listas (ACL) de autorización, configure una zona segura, etc.-, y protéjase sobre todo, contra cualquier tipo de consulta de transferencia de zona que aunque le pueda parecer que cualquier administrador de sistemas debería tener en cuenta o prevenir esta circunstancia, no siempre es así. La configuración de este tipo de servidor DNS u otros similares escapa al ámbito de este libro, por lo que le aconsejo que se documente y profundice en el tema ya que la seguridad de su infraestructura dependerá de estos y otros factores.

Resolverdb3.py

```
#!/usr/bin/env python
# -*- coding: latin-1 -*-
#Versión:Python 2.7.6
#Check 07/04/2014
#Sistema:Backtrack5_release_10.04
#Kernel:linux 2.6.38
#Puede copiar,modificar y publicar este codigo en el medio que desee #haciendo referencia de origen al autor del mismo.
#Utilice el mismo con responsabilidad en entornos seguros y controlables

import os,sys,commands

def directo():
    origen = open('nombreserv.txt','r')
    filtradodirecto = open('filtradodirecto.txt','w+')
    maquinas = origen.readlines()

    for host in maquinas[:-1]:
```

```
        resolucion = os.system ("host %s.%s > /dev/null" % (host[0:-1],dominio))
        if ( resolucion == 0 ) :
                resultado = commands.getoutput("host %s.%s" % (host[0:-1],dominio))
                filtradodirecto.write(resultado.replace("%s.%s has address " % (host[0:-1],dominio),"") + "\n")
                print resultado.replace("%s.%s has address " % (host[0:-1],dominio),"")

    origen.close()
    filtradodirecto.close()
    return;


def ocultos():
    filtradoinverso = open('filtradoinverso.txt','w+')
    filtradons = open('filtradozonas.txt','w+')
    print ("[Este proceso no aisla nodos o duplicidades IP]")
    print ""

    for equipo in range(255):
      resolucioninversa = os.system("host 192.168.1.%s > /dev/null" % (equipo))


    if ( resolucioninversa == 0 ) :
          resultadoinverso = commands.getoutput("host 192.168.1.%s" % (equipo))
          inicial = resultadoinverso.find("pointer")
          filtradoinverso.write("192.168.1.%s : %s" % (equipo,resultadoinverso[(inicial + 8):-1]) + "\n")
          print ("192.168.1.%s : %s" % (equipo,resultadoinverso[(inicial + 8):-1]))     maquinadominio =
          (resultadoinverso[(inicial + 8):-1])

          if ( maquinadominio.find("ns")!= -1 ):
              filtradons.write("%s" % (resultadoinverso[(inicial + 8):-1]) + "\n")

    filtradoinverso.close()
    filtradons.close()
    return;


def transzona(dominio):
    filtradons = open('filtradozonas.txt','r+')
    maquinasns = filtradons.readlines()
    print ("[automático 0--->9 (NS)")
    print ""

    for nombresns in maquinasns :
        print ("%s" % (nombresns))
        print ""
        copyzona = os.system ("host -l %s %s.centraltermica.lan > /dev/null" % (dominio,nombresns[0:3]))

        if ( copyzona == 0 ) :
            filtradons.write(commands.getoutput("host -l %s %s.centraltermica.lan" % (dominio,nombresns[0:3])))
            print (commands.getoutput("host -l %s %s.centraltermica.lan" % (dominio,nombresns[0:3])))

    filtradons.close()
    return;


os.system ("clear")
print ""
print ("Versión: Free")
print ("Check 07/04/2014")
print ""
print ("[Herramienta sin optimizar para estudio_(práctica 12)]")
print ""
dominio = raw_input("Dominio: ")
print ""
print ("ANÁLISIS POR DICCIONARIO...")
print ("**************************")
print ""
directo();
print ""
print ("ANÁLISIS INVERSO DE HOSTS OCULTOS...")
print ("***********************************")
print ""
ocultos();
print ""
print ("SERVIDORES DE NOMBRES (ns) Y TX ZONA...")
print ("***************************************")
```

```
print ""
transzona(dominio);
print ""
```

Reinicie el servidor DNS y ejecute la herramienta especificando el dominio local ..

```
root@lab:/# /etc/init.d/bind9 restart

root@lab:/# python resolverdb3.py


Versión: Free
Check 07/04/2014

Esta herramienta es didáctica y forma parte del libro
y curso avanzado de Hacking y Seguridad Informática

[Herramienta sin optimizar para estudio]

Dominio: centraltermica.lan


ANÁLISIS POR DICCIONARIO... **************************

192.168.1.34
192.168.1.250
192.168.1.106
192.168.1.107
192.168.1.108
192.168.1.100
192.168.1.109
192.168.1.200
192.168.1.105
192.168.1.101
192.168.1.102
192.168.1.103
192.168.1.104

ANÁLISIS INVERSO DE HOSTS OCULTOS...
***********************************

[Este proceso no aisla nodos o duplicidades IP]

192.168.1.34 : ns1.centraltermica.lan
192.168.1.100 : ftp.centraltermica.lan
192.168.1.101 : administracion.centraltermica.lan
192.168.1.102 : contabilidad.centraltermica.lan
192.168.1.103 : facturacion.centraltermica.lan

. . .

192.168.1.243 : imagen1.centraltermica.lan
192.168.1.244 : imagen2.centraltermica.lan
192.168.1.245 : backupconfig.centraltermica.lan
192.168.1.246 : resets.centraltermica.lan
192.168.1.247 : remoto2.centraltermica.lan
192.168.1.250 : www.centraltermica.lan

SERVIDORES DE NOMBRES (ns) Y TX ZONA...
***************************************

[automático 0--->9 (NS)

ns1.centraltermica.lan

Using domain server:
Name: ns1.centraltermica.lan
Address: 192.168.1.34#53

Aliases:

centraltermica.lan name server ns1.centraltermica.lan.
administracion.centraltermica.lan has address 192.168.1.101
```

backup.centraltermica.lan has address 192.168.1.104
contabilidad.centraltermica.lan has address 192.168.1.102
facturacion.centraltermica.lan has address 192.168.1.103
fichastecnicas.centraltermica.lan has address 192.168.1.105
ftp.centraltermica.lan has address 192.168.1.100
login.centraltermica.lan has address 192.168.1.109
mail1.centraltermica.lan has address 192.168.1.106
mail2.centraltermica.lan has address 192.168.1.107
mail3.centraltermica.lan has address 192.168.1.108
ns1.centraltermica.lan has address 192.168.1.34
router.centraltermica.lan has address 192.168.1.200
www.centraltermica.lan has address 192.168.1.250

(*)Referencias

Autor: José Luis Prado Seoane
Freelance especializado en Seguridad Informática y Electrónica de sistemas y/o dispositivos en los entornos empresariales.
Blog: joseluispradoseoane.wordpress.com

(*)Comunidad

Compartir parte de tu trabajo y tiempo con la comunidad técnica (Researchers), sectores académicos, sectores profesionales de la seguridad, empresas del sector o con todos aquellos interesados en este mundo, etc.-, hace que el Hacking Ético bien enfocado adquiera su verdadero significado o sentido aportando un nuevo valor añadido a la seguridad en los entornos empresariales.

Dominio estudio

Dominio utilizado para la realización de este PaperLab: centraltermica.lan
(el mismo es local/Ip´s y permite presentar el desarrollo del proceso de una forma ordenada y segura)

ADVERTENCIA

“ Actúe siempre con responsabilidad y recuerde, la finalidad es siempre el aprendizaje y la adquisición de conocimientos para la protección de los entornos informáticos en el ámbito de la empresa o la Ciberseguridad“

Joseluispradoseoane.wordpress.com