**Gathering Information**

Mantener a salvo la información es imperativo y primordial en cualquier empresa. La confidencialidad de sus datos es ineludible para mantener una buena política de seguridad.

Gracias a la recolección de información, muchos ataques a empresas acaban con éxito.

Como podemos intuir toda fase de ataque a un determinado objetivo su primer paso a realizar es la recolección de información, o más conocido como “Information Gathering”. Este proceso es el menos atractivo para el atacante ya que sólo radica en acumular información.

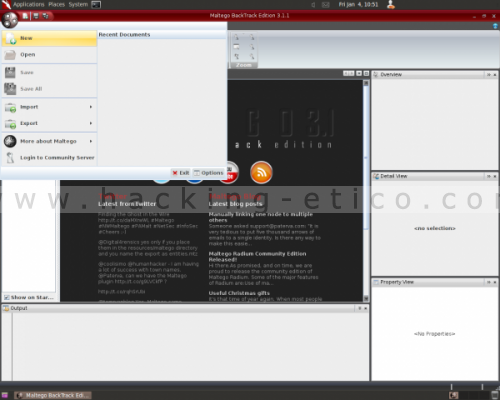
Durante este primer tramo del ataque, el atacante usando diferentes técnicas y/o aplicaciones para tal fin, obtiene direcciones IP, servicios de equipos, nombres de dominio, metadatos, sistemas operativos, y un largo etcétera.

Una de estas aplicaciones para obtener información es MALTEGO. Es una aplicación muy amigable, fácil de entender y con interfaz gráfica (GUI). Ideal para la fase de “Information Gathering”.

Para su uso es imprescindible registrarse en la Web de la empresa desarrolladora. No os preocupéis ya que es un registro muy rápido, sencillo y gratis. El software está disponible para Windows, Linux y Mac. En nuestro caso lo hemos usado con la distribución BACKTRACK 5 R3.

Una vez iniciado el programa te pedirá el registro en la Web, basta con entrar los datos de registro y el CAPTCHA para poder usar el programa.

Nada mas iniciar el programa debemos clickar donde muestra la imagen, en la esquina superior izquierda, para abrir una nueva “Palette”.



Elegiremos, por ejemplo, la opción “Domain”, arrastrando el icono a la parte central de la pantalla. Una vez colocado en el centro de la pantalla, pulsaremos F2 para cambiarle el dominio del objetivo, en nuestro caso “hacking-etico.com”.

Ahora situándonos encima del icono con nuestro dominio de prueba, hacemos clic con el botón derecho, eligiendo del menú contextual que nos aparece, la opción: “Run Transform > DNS From Domain > All in this test” Con esta opción nos mostrará los servidores DNS del dominio analizado.

Tiene también opción de usarse para cuentas Twitter y Facebook aunque son un poco más tediosas de hacerlas funcionar por su interacción y seguridad con sus servidores.

Y recordad, entre más información se recopile, más facilidad se obtendrá a la hora de atacar un objetivo, incluso con información que la empresa crea que no es útil para ataques.

**Routing And Switching**

El funcionamiento de una red consiste en conectar computadoras y periféricos mediante dos partes del equipo: switches y routers. Estos dos elementos permiten a los dispositivos conectados a la red comunicarse con los demás y con otras redes. Aunque son muy parecidos, los switches y routers realizan funciones muy diferentes en la red:

Los Switches se utilizan para conectar varios dispositivos a través de la misma red dentro de un edifcio u ofcina. Por ejemplo, un switch puede conectar sus computadoras, impresoras y servidores, creando una red de recursos compartidos. El switch actuaría de controlador, permitiendo a los diferentes dispositivos compartir información y comunicarse entre sí. Mediante el uso compartido de información y la asignación de recursos, los switches permiten ahorrar dinero y aumentar la productividad. Existen dos tipos básicos de switches: administrados y no administrados. Los switches no administrado funcionan de forma automática y no permiten realizar cambios. Los equipos en redes domésticas suelen utilizar switches no administrados. Los switches administrados permiten su programación. Esto proporciona una gran fexibilidad porque el switch se puede supervisar y ajustar de forma local o remota para proporcionarle control sobre el desplazamiento del tráfco en la red y quién tiene acceso a la misma.

Los routers se utilizan para conectar varias redes. Por ejemplo, puede utilizar un router para conectar sus computadoras en red a Internet y, de esta forma, compartir una conexión de Internet entre varios usuarios. El router actuará como distribuidor, seleccionado la mejor ruta de desplazamiento de la información para que la reciba rápidamente. Los routers analizan los datos que se van a enviar a través de una red, los empaquetan de forma diferente y los envían a otra red o a través de un tipo de red distinto. Conectan su negocio con el mundo exterior, protegen la información de amenazas a la seguridad e, incluso, pueden decidir qué computadoras tienen prioridad sobre las demás

**DMITRY**

Dmitry tiene la capacidad de dar tanta información como sea posible sobre un host. Se puede utilizar para realizar búsquedas de Internet, whois, recuperar la hora del sistema y los datos del servidor. La capacidad de realizar búsquedas de subdominios en un objetivo.

También realiza la exploración de los puertos TCP.

**Sintaxis**

* ***Dmitry [ -winsepfb] [ -t 0-9] [ -o %host.txt] host***

**Opciones**

* **-o** nos permite especificar un nombre dado a nuestra salida el valor predeterminado es host.txt usted podría nombrar lo que quieras.
* **-i** nos permite realizar una búsqueda whois de la dirección IP de un host, esto nos dice que si nosotros no sólo el nombre que se encuentra el dmitry IP para nosotros.
* **-w** realizará una búsqueda whois sobre el nombre de dominio de un huésped.
* **-n** nos dará información [Netcraft.com](http://netcraft.com/) en una máquina (si usted no sabe acerca de [netcraft.com](http://netcraft.com/) luego ir a tomar una mirada que usted no será decepcionado).
* **-s** realiza una búsqueda de posibles subdominios ([www.yourexampleofanetwork.com](http://www.yourexampleofanetwork.com/) ser un dominio de nivel superior y [www.yoursitexample.yourexampleofanetwork.com](http://www.yoursitexample.yourexampleofanetwork.com/) ser un subdominio.)
* **-e** realizará una búsqueda de direcciones de correo electrónico posibles. (Youremail@yournetwork.com)
* **-p** llevará a cabo un escaneo de puertos TCP en un host
* **-f**llevará a cabo un escaneo de puertos TCP en un host que muestra los puertos de salida de informes filtrados (útil si hay un cortafuegos en su lugar)
* **-b** se informe a una bandera recibida de un puerto de la máquina (Tenga en cuenta que esto sólo funcionará si el puerto nos envía una bandera cuando se escanea).   
  (Esto puede revelar algún tipo de software que se ejecuta en un puerto determinado.)
* **-T 0-9** se utiliza para establecer el TTL en cuestión de segundos cuando se explora el valor por defecto es 2

El \* significa que la opción-p también se debe configurar para que funcione.

**Ejemplo**

* ***dmitry-winsepffb-o hosts.txt***[***www.yourexampleofanetwork.com***](http://www.yourexampleofanetwork.com/)  
    
  HostIP: 192.168.1.1   
  HostName: [www.yourexampleofanetwork.com](http://www.yourexampleofanetwork.com/)
* A continuación:

Reunidos Inet-whois información para 192.168.1.1   
A continuación, debería ver:   
  
Reunidos INIC-whois información para [www.yourexampleofanetwork.com](http://www.yourexampleofanetwork.com/)   
---------------------------------   
Nombre de dominio: [YOUREXAMPLEOFANETWORK.COM](http://yourexampleofanetwork.com/)   
Secretario: La información aquí Registradores   
Whois Server: [whois.example.com](http://whois.example.com/)   
URL de referencia: [http://www.example.com](http://www.example.com/)   
Nombre del servidor: [NS1.YOUREXAMPLEOFANETWORK.COM](http://ns1.yourexampleofanetwork.com/)   
Nombre del servidor: [NS2YOUREXAMPLEOFANETWORK.COM](http://ns2yourexampleofanetwork.com/)   
Nombre del servidor: [NS3.YOUREXAMPLEOFANETWORK.COM](http://ns3.yourexampleofanetwork.com/)   
Nombre del servidor: [NS4.YOUREXAMPLEOFANETWORK.COM](http://ns4.yourexampleofanetwork.com/)   
Estado: clientDeleteProhibited   
Estado: clientTransferProhibited   
Estado: clientUpdateProhibited   
Fecha Actualización: 10-abril-2006   
Fecha de creación: 15-septiembre-1997   
Fecha de Vencimiento: 14-septiembre-2011   
>>> Última actualización de base de datos whois: Sun, 23 de diciembre 2007 06:42:27 UTC   
De nuevo, esto proporciona más información acerca de nuestra red de destino. Ahora tenemos los servidores de nombres, así como el nombre del registrador.   
Todo esto es muy útil cuando estamos "reconning" nuestro objetivo.   
Siguiente netcraft con:   
  
La información obtenida por Netcraft [www.yourexampleofanetwork.com](http://www.yourexampleofanetwork.com/)   
---------------------------------   
Recuperación de información [Netcraft.com](http://netcraft.com/) para [www.yourexampleofanetwork.com](http://www.yourexampleofanetwork.com/)   
Sistema operativo: Winblows servidor edition2007   
WebServer: winblowswebserver v1.0   
No hay informes disponibles para el tiempo de actividad de acogida: [www.yourexampleofanetwork.com](http://www.yourexampleofanetwork.com/)   
Información recopilada [Netcraft.com](http://netcraft.com/)   
  
Ahora bien, si nuestra red objetivo estaba usando algo que no sea el servidor de mal codificados Winblows Edition 2007   
Entonces es posible que no se presenta aquí por nosotros. Lo mismo con la información de servidor web.   
Y como está tan mal codificados, vemos que no hay tiempo de actividad ya que es sólo en alrededor de una hora antes de un reinicio es necesario.   
  
La información obtenida Subdominio para [www.yourexampleofanetwork.com](http://www.yourexampleofanetwork.com/)   
---------------------------------   
Búsqueda [Google.com](http://google.com/): 80 ...   
HostName: [images.yourexampleofanetwork.com](http://images.yourexampleofanetwork.com/)   
HostIP: 192.168.1.2   
HostName: [maps.yourexampleofanetwork.com](http://maps.yourexampleofanetwork.com/)   
HostIP: 192.168.1.3   
HostName: [news.yourexampleofanetwork.com](http://news.yourexampleofanetwork.com/)   
HostIP: 192.168.1.100   
HostName: [www.yourexampleofanetwork.com](http://www.yourexampleofanetwork.com/)   
HostIP: 192.168.1.1   
HostName: [mail.yourexampleofanetwork.com](http://mail.yourexampleofanetwork.com/)   
HostIP: 192.168.1.5   
Encontradas 5 posibles subdominio (s) para el anfitrión [yourexampleofanetwork.com](http://yourexampleofanetwork.com/), buscado 1 páginas contienen un resultado.   
Y así sucesivamente hasta que se ha buscado a través de todos los subdominios que encuentre.   
A continuación vamos a ver:   
  
Reunidos E-Mail información para [yourexampleofanetwork.com](http://yourexampleofanetwork.com/)   
administración ATyourexampleofanetwork DOT com   
joeuser AT yourexampleofanetwork DOT com   
  
Y finalmente la salida de nuestra TCP scan   
  
Reunidos Puerto TCP información para 192.168.1.1   
---------------------------------   
Estado rector del puerto   
20 Open   
Abierto 21   
Abierto 80   
Etc, Etc, Etc, Etc   
  
Porque [www.yourexampleofanetwork.com](http://www.yourexampleofanetwork.com/) está ejecutando el servidor Winblows edición de 2007 y dejó a todos los puertos comunes, ofrecen por defecto!   
Así que espero que este tutorial se va y usted puede comenzar a usar dmitry hacer algo de "reconning".   
  
BTW Todos los nombres y direcciones IP y correos electrónicos han sido cambiados para proteger a mí.  
Si usted alimenta a números de bloque como privados. 192 A continuación, el dato de whois le dirá que es para uso de red interno.   
La única parte útil de todo el escaneo será el escaneo de puertos.