ACTIVIDAD NÚMERO 2

Daniel Santacruz

Carlos López

Presentado a:

Arturo Erazo

Consulta DNS e introducción a Kali linux

INSTITUCIÓN UNIVERSITARIA CESMAG
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2017

Actividad No 2. DNS

1. Que es un DNS? Que puerto trabaja.
2. Cómo trabaja un DNS? Explique.
3. Explique que son los registros: NS, A, MX, CNAME, SOA. De un ejemplo de cada caso.
4. Consulte en kali linux, en que consisten y como trabajan: dnsrecon y fierce. De un ejemplo de cada caso e interprete la información.

1. Que es un DNS? Que puerto trabaja.

El sistema de nombres de dominio (DNS, por sus siglas en inglés, Domain Name System) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. es una tecnología basada en una base de datos que sirve para resolver nombres en las redes, es decir, para conocer la dirección IP de la máquina donde está alojado el dominio al que queremos acceder

Este sistema asocia información variada con nombre de dominio asignado a cada uno de los participantes.

los DNS únicamente son unas direcciones que introducimos en nuestra configuración de conexión a Internet y que nos sirven para poder conectarnos y para otros, son esas “cosas” que tienen que expandirse para que una dirección nueva se pueda ver en todas las conexiones.

Cuando un ordenador está conectado a una red (ya sea Internet o una red casera) tiene asignada una dirección IP. Si estamos en una red con pocos ordenadores, es fácil tener memorizadas las direcciones IP de cada uno de los ordenadores y así acceder a ellos pero ¿qué ocurre si hay miles de millones de dispositivos y cada uno tiene una IP diferente? Pues que se haría imposible, por eso existen los dominios y las DNS para traducirlos.

Cliente DNS: está instalado en el cliente (es decir, nosotros) y realiza peticiones de resolución de nombres a los servidores DNS.

Servidor DNS: son los que contestan las peticiones y resuelven los nombres mediante un sistema estructurado en árbol. Las direcciones DNS que ponemos en la configuración de la conexión, son las direcciones de los Servidores DNS.

Zonas de autoridad: son servidores o grupos de ellos que tienen asignados resolver un conjunto de dominios determinado (como los .es o los .org).

Los servicios de un Domain Name Server utilizan el puerto 53 en UDP y también en TCP para hacer zone transfers (axfrs).

2_ Cómo trabaja un DNS? Explique

Todos los nombres de DNS son escritos con una jerarquía específica que se divide en tres partes: el host (anfitrión o servidor), el dominio, y el dominio de nivel superior (Top Level Domain -TLD). Por ejemplo, en www.bitelia.com, www es el host, .bitelia es el dominio, y .com es el TLD. Todos los dominios necesitan estar registrados bajo un TLD, ya sea .org, .net, .com, etc. Un subdominio es opcional y va a la izquierda del nombre de dominio, el dueño del mismo es libre de de crear subdominios y mantenerlos en el mismo servidor.

Cada dominio o subdominio tiene una o más zonas de autoridad que publican la información acerca del dominio y los nombres de servicios de cualquier dominio incluido. La jerarquía de las zonas de autoridad coincide con la jerarquía de los dominios. Al inicio de esa jerarquía se encuentra los servidores raíz: los servidores que responden cuando se busca resolver un dominio de primer y segundo nivel

Cuando un usuario abre el navegador y escribe una dirección, se desencadenan una serie de eventos que aunque implican una cadena bastante larga de dominós, frente a tus ojos ocurren en apenas un instante.

Primero el ordenador revisa su propio caché de DNS en busca de la dirección IP (si ya has entrado antes a un sitio, la segunda siempre es más rápida porque queda almacenado en la memoria caché o temporal), si no la consigue se reenvía la petición al servidor de DNS local (este es usualmente el de tu ISP si nunca lo has cambiado).

Ahora los servidores DNS locales verifican su propia caché para buscar la dirección IP y comprobar si ya conocen la respuesta, y si no lo consiguen entonces reenvían la petición a los servidores raíz del dominio (esto es lo que se conoce como búsqueda recursiva), y estos responden con la información.

Luego el servidor DNS local reenvía la información que obtuvo de los servidores raíz con la dirección IP para el host, y almacena en caché la información para el futuro. La computadora del usuario hace lo mismo, y por último el navegador genera una petición HTTP al servidor WWW de unsitiowebcualquiera.com localizado en la dirección IP 001.000.000.111. El servidor WWW responde la petición y le envía la página web al usuario.

3_ Explique que son los registros: NS, A, MX, CNAME, SOA. De un ejemplo de cada caso

Registro SOA, es el Registro de “Start of Authority” para un dominio. Contiene identificadores del servidor de nombres con autoridad sobre la denominación y su operador, y diversos contadores que regulan el funcionamiento general del sistema de nombres de dominio (DNS) para la denominación. Todo servidor de

nombres de una denominación debe responder a una consulta por el registro SOA de esa denominación en forma autoritativa.

Además escribe los valores por defecto para el resto de parámetros de registro SOA en los archivos de zona que mantiene.

Dentro de los valores SOA se pueden configurar varios parámetros de opciones.

- TTL. Esto es el tiempo que los servidores DNS deben guardar el registro en el caché. Plesk establece el valor por defecto de un día.
- Actualizar. Esto es la frecuencia con la que los servidores de nombres secundarios verifican el servidor de nombres primarios para ver si se han realizado cambios en el archivo de zona de dominio. Plesk establece el valor por defecto de tres horas.
- Volver a Intentar. Esto es el tiempo que un servidor secundario espera para recuperar una transferencia de zona fallida. Este tiempo suele ser menor al intervalo de actualización. Plesk establece el valor por defecto de una hora.
- Expirar. Esto es el tiempo antes que un servidor secundario deje de responder a las búsquedas una vez se haya producido un intervalo de actualización de la zona. Plesk establece el valor por defecto de una semana.
- Mínimo. Esto es el tiempo en que un servidor secundario debe cachear una respuesta negativa. Plesk establece el valor por defecto de tres horas.
- Número de Serie: Puede estar en varios formatos, tanto en IETF o en Unix-timestamp (menos utilizado).
- Persona responsable: Contiene la dirección de correo electrónico de la persona responsable donde la @ es un . (punto).
- Propietario: Es el nombre de dominio de la zona.

El uso del formato de número de serie recomendado por IETF y RIPE es obligatorio para muchos dominios registrados en algunas zonas DNS de alto nivel, mayoritariamente europeas. Si su dominio está registrado en una de estas zonas y su registrador no acepta su número de serie SOA, el uso del formato de número de serie recomendado por IETF y RIPE debería solucionar esta incidencia.

Los servidores que usan la sintaxis UNIX-timestamp para configurar zonas DNS. UNIX timestamp es el número de segundos desde el 1 de enero del 1970 (Unix Epoch). El timestamp 32-bit finalizará el 8 de julio del 2038.

RIPE recomienda usar el formato YYYYMMDDNN , donde YYYY es el año (cuatro dígitos), MM es el mes (dos dígitos), DD es el día del mes (dos dígitos)

y nn es la versión para día (dos dígitos). El formato YYYYMMDDNN no finalizará hasta el año 4294.

Registro CNAME (Canonical Name) es un tipo de registro que puede encontrarse en un DNS y que permite al usuario especificar el alias de un nombre de dominio. Por ejemplo, podemos crear un alias para dominio1.com con dominio2.com. De todos modos, lo típico es emplearlo para crear alias de subdominios, incluyendo los más comunes, que obviamente son “www”.

A menudo un registro de dominio establecido por defecto lleva un comodín (*) que resolverá cualquier subdominio, incluidos los “www”. Si no lo hace, necesitará algo como esto:

www.dominio1.com CNAME dominio1.com

También podemos hacer que uno apunte al otro con:

ftp.dominio1.com. CNAME sftp.dominio1.com.

Siguiendo la misma línea, muchos servidores de email emplean los subdominios de la siguiente manera:

mail.dominio1.com. CNAME dominio1.com.

Los registros CNAME son también muy útiles cuando apuntan a dominios externos, particularmente cuando se usan servicios de computación en nube como es el caso de Google Maps La particularidad de usar CNAME reside en que permite distinguir eficazmente que el servicio en cuestión pertenece a otro dominio.

Registro MX (Mail Exchanger) especifican y priorizan los servidores de correo entrante que recibe mensajes enviados a su nombre de dominio. Con frecuencia, no es necesario modificar sus registros MX. A veces tendrá que actualizarlos si aloja un sitio web con una red pero tiene su correo electrónico en otra.

Normalmente, tiene varios registros MX asignados para su nombre de dominio, lo cual puede prevenir que los mensajes de correo se pierdan durante una interrupción de energía. Cada registro MX tiene una prioridad o un número para designar el orden en que los servidores de correo entrante de su nombre de dominio reciben sus mensajes. El registro MX con el menor número es el servidor de correo primero o primario, cuyos servidores de correo saliente intentarán enviar sus mensajes.

Por ejemplo, si tiene MX0 y MX10, entonces MX0 es su servidor de correo primario y MX10 es su servidor alternativo. Si no está disponible su servidor de correo primario, el servidor alternativo almacenará sus mensajes hasta que su servidor primario vuelva a operar.

Podrá hacer clic en Restore Defaults en la sección MX (Mail Exchanger) del Editor de Archivos de Zona para restablecer los registros MX predeterminados de su nombre de dominio. Para más información.

Registro NS. (Name Server)

Contiene los servidores de nombre de ese dominio, lo que permite que otros servidores de nombres vean los nombres de su dominio.

Registro A

Los registros de dirección A, (Adress) asocian nombres de host a direcciones IP dentro de una zona. Son los más numerosos dentro del archivo.

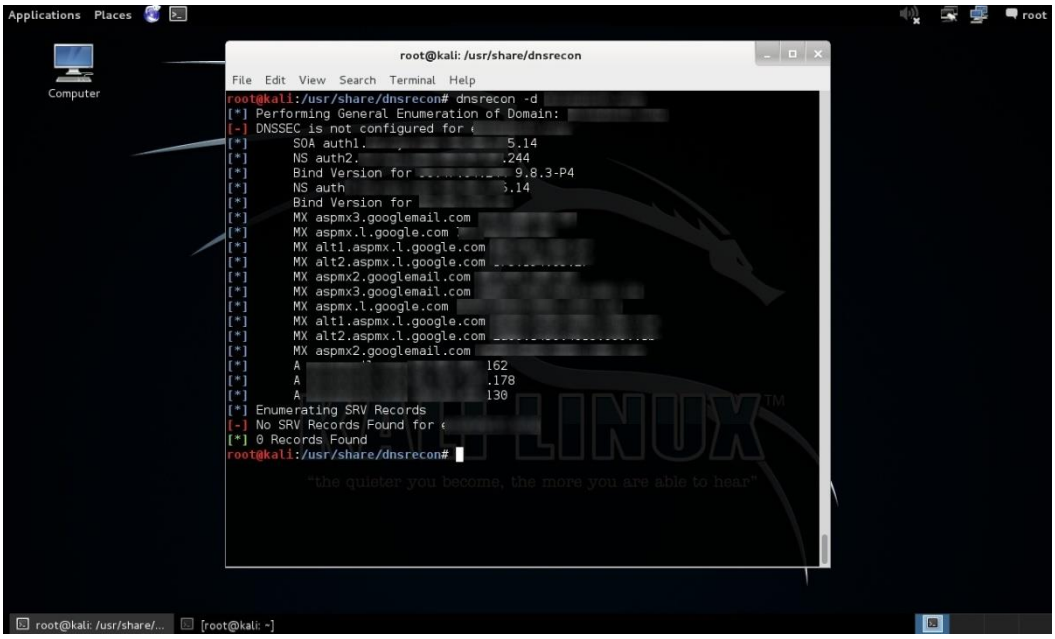
Es a donde va a ir el dominio cuando lo invoques y tiene que ser una dirección IP. Para que te hagas una idea, cuando escribes rubenmartin.me a que dirección/máquina desea que vaya a resolver la petición.
La diferencia entre A y AAAA, es que la primera es para IPv4 y la segunda para IPv6, pero tienen el mismo comportamiento.

4_Consulte en kali linux, en qué consisten y como trabajan: dnsrecon y fierce. De un ejemplo de cada caso e interprete la información.

DNSRecon es una herramienta de escaneo y enumeración DNS escrita en Python, la cual permite realizar diferentes tareas, como enumeración de registros estándar para un dominio definido (A, NS, SOA y MX). Expansión de dominio de nivel superior para un dominio definido. Transferencia de zona contra todos los registros NS para un dominio definido. Consulta reversa contra un rango de direcciones IP, proporcionando una dirección IP inicial y final.

La manera más simple de utilizar dnsrecon es definiendo el dominio del objetivo de evaluación utilizando la opción “-d”. Si no se especifica la opción “-n” o servidor de nombres a utilizar, se utilizará el SOA del objetivo.

dnsrecon -d xxxxx .com



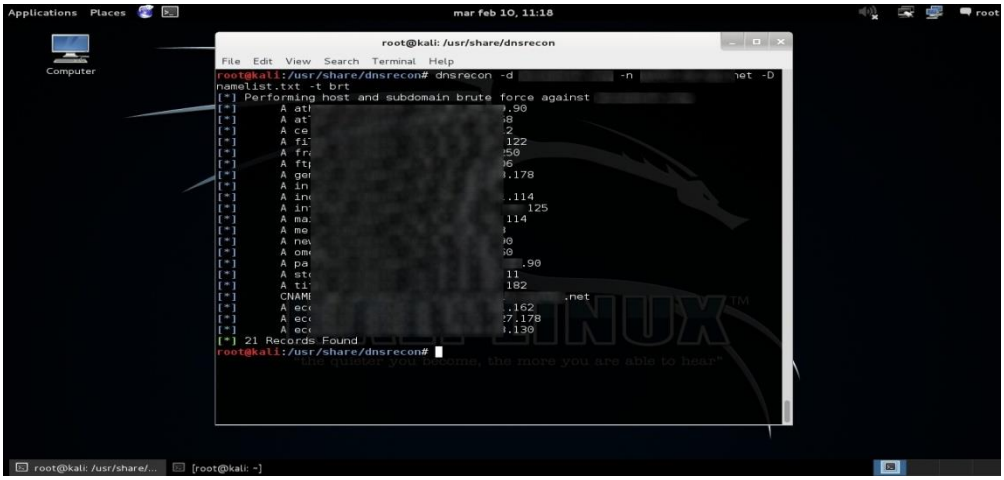
Obtenidos los servidores de nombres, se procede a realizar una enumeración por fuerza bruta.

La opción “-n” define el servidor de dominio a utilizar.

La opción “-D” define el archivo Diccionario de sudominios o nombres de host a utilizar para la fuerza bruta.

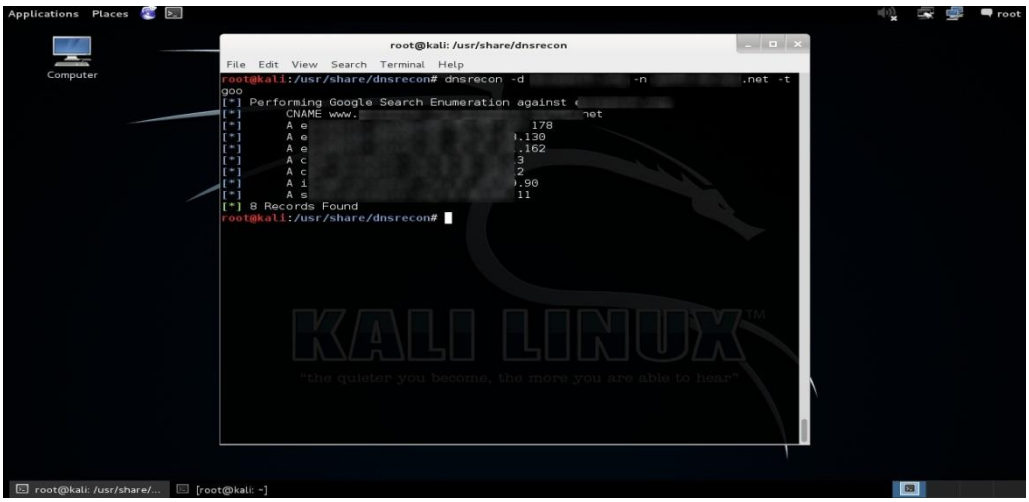
La opción “-t brt” especifica el tipo de enumeración a realizar, “brt” es para realizar fuerza bruta de dominios y host utilizando un diccionario definido.

dnsrecon -d xxxxx .com -n dns1. xxxxx. com -D namelist.txt -t brt



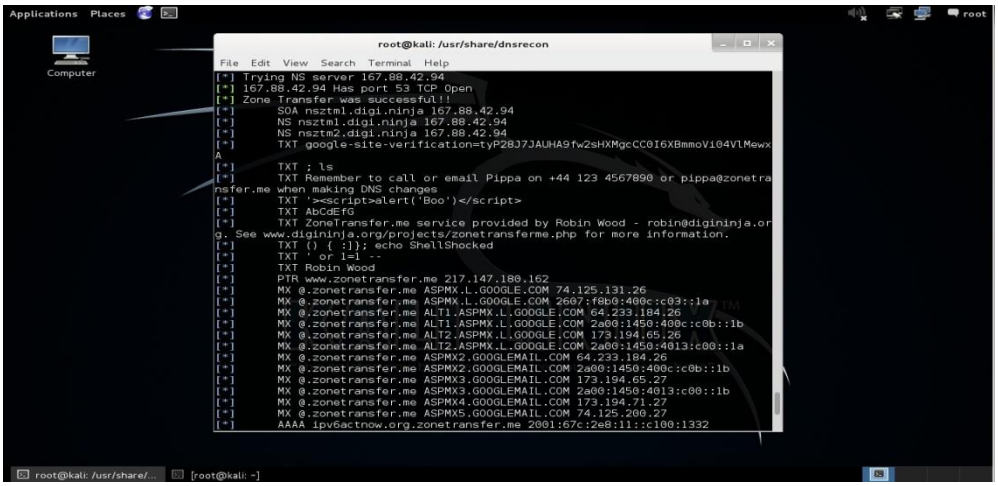
Es factible utilizar el motor de búsqueda Google para realizar una búsqueda de subdominios y hosts. Para esto se utiliza la opción “-t goo”

dnsrecon -d xxxxx .com -n dns1. xxxxx .com -t goo



Para la siguiente demostración se utiliza el dominio, zonetransfer.me cuyos servidores de nombres permiten realizar transferencias de zona satisfactorias.

dnsrecon -d zonetransfer.me -t axfr



Fierce: Fierce es una escáner semi ligero para realizar una enumeración que ayude a los profesionales en pruebas de penetración a localizar espacios IP y nombres de host no continuos para dominios específicos, utilizando cosas como DNS, Whois y ARIN.

Para la siguiente práctica se utilizará la versión de Fierce v2.0 incluida en Kali Linux.

La manera más sencilla de ejecutar Fierce es utilizando la opción “-dns” seguida del dominio objetivo a escanear. Este puede ser un único dominio, varios dominios (separados por comas), o un archivo conteniendo un dominio por linea. La opción “-dnsservers” define un servidor DNS en particular para realizar las consultas, se puede definir también varios servidores o un archivo conteniendo una lista de servidores DNS. La opción “-format” define el formato del archivo conteniendo los resultados, y la opción “-output” define el nombre archivo donde se guardarán los resultados obtenidos por Fierce.

fierce2 -dns [Dominio Objetivo] -dnsservers [DNS Objetivo] -format html -output /tmp/resultadouy.html

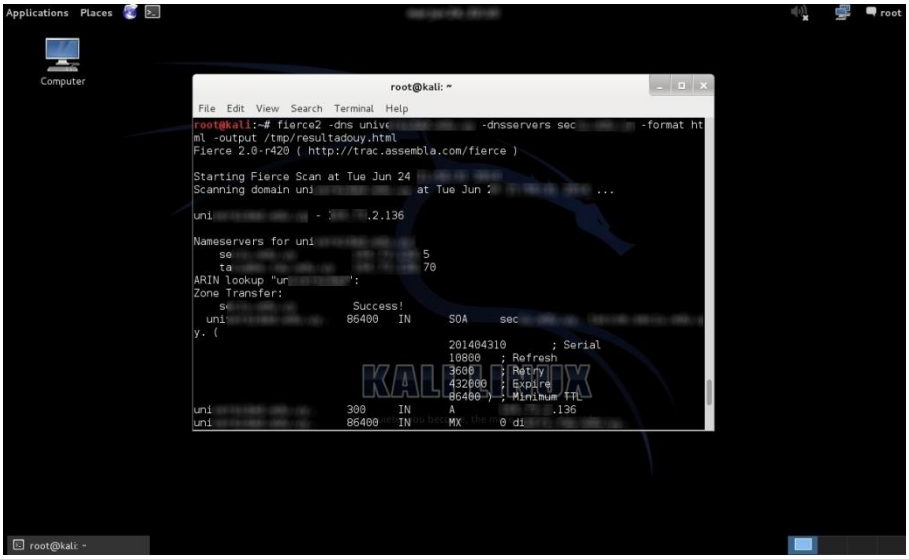
Fierce utiliza varias técnicas para identificar potenciales objetivos para la Prueba de Penetración. Estas pruebas son en principio pasivas por naturaleza; dado que no tendrán ningún impacto negativo, pues la mayoría técnicas incluyen consultas DNS y búsquedas ARIN no intrusivas.

Enumerar los servidores de nombres

Cuando Fierce inicia un escaneo contra un dominio, primero resuelve el dominio a direcciones IP. Luego continua con la identificación de los servidores de nombres primario, secundario, o adicionales. Estas peticiones son conocidas como “peticiones NS” el cual es una abreviatura para “servidores de nombres”. Estos servidores pueden contener información adicional sobre el objetivo que no está disponible a través de servidores DNS públicos, así una vez identificados los servidores de nombres por Fierce para un dominio objetivo, usará estos servidores para todas las peticiones DNS futuras.

ARIN

Una de las nuevas características en Fierce 2.0 es el módulo ARIN. Cuando es utilizado, Fierce 2.0 realizará primero una búsqueda ARIN del dominio. El resultado de esta consulta contendrá varios manejadores de red. Cada uno de estos son luego consultados para obtener más detalles sobre los rangos que son propiedad del dominio en evaluación.



Transferencia de Zona

Fierce aprovecha una técnica clásica de reconocimiento pasivo para identificar información desde los servidores de nombres para un dominio objetivo. Intentará una “petición AXFR” contra cada servidor de nombres. Si una de estas peticiones es satisfactoria, Fierce continuará realizando peticiones AXFR contra todos los servidores de nombres, dado que los servidores DNS algunas veces se configuran de manera diferente. No es improbable para una organización exponer direcciones IP internas (RFC 1918) a través de estos archivos de zona, lo cual puede ser muy útil en la determinación de hosts objetivos una vez que el atacante gana acceso interno. Usualmente no existe razón para que una organización tenga habilitado permanentemente la transferencia de zona. Por lo tanto, se recomienda deshabilitarla en todos los servidores de nombres.

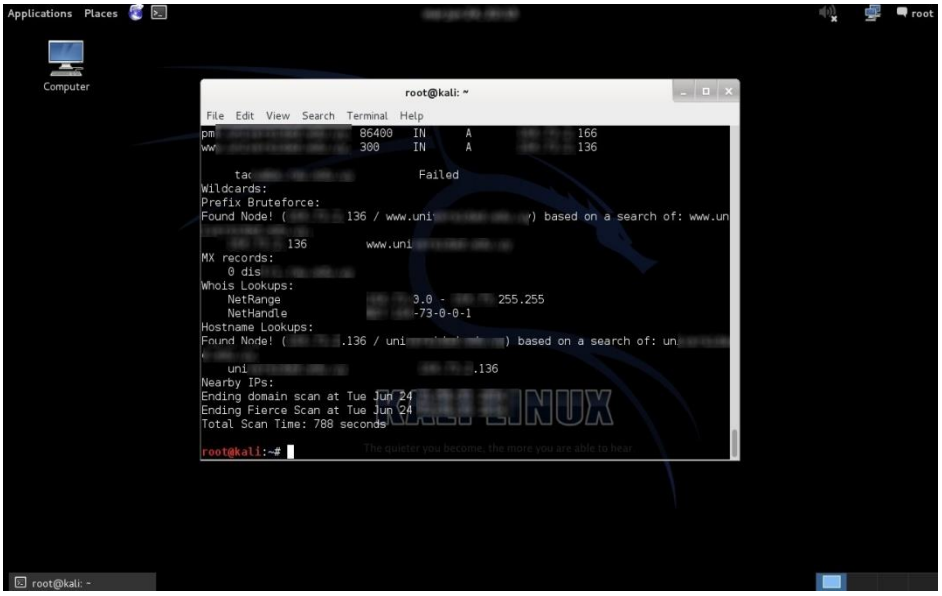
Registros DNS Comodín

La siguiente técnica que Fierce utiliza para identificar direcciones IP para un dominio objetivo es verificar por registros DNS Comodín. Este es un paso importante, si la organización tiene un comodín puesto que puede afectar el resto de la prueba. Por ejemplo, algunas organizaciones configuran los servidores DNS para resolver cualquier subdominio hacia una dirección IP específica. Si este es el caso, el analista debe tener en mente que cualquier nombre de host resolverá a esta dirección IP, esto probablemente debido al uso del comodín, no debido a la validez del nombre del host. El analista debe considerar esto cuando se realiza el reconocimiento de la red, personalizando las pruebas para identificar objetivos adicionales y prevenir falsos positivos.

Fuerza Bruta de Prefijos

La Fuera Bruta de Prefijos es una técnica utilizada para localizar nombres de host que resuelven hacia una dirección IP. Fierce intenta técnicas avanzadas para realizar fuerza bruta de prefijos, ademas de intentar resolver prefijos comunes como (www, mail, test). Fierce intentará añadir dígitos desde el 1 hasta al 5 al final de cada prefijo para identificar sistemas adicionales asociados con este prefijo.

Adicionalmente Fierce realiza búsquedas para enumerar todos los registros MX para un dominio. Tiene la habilidad de realizar búsquedas Whois contra las direcciones de un dominio. Fierce también realiza búsquedas para todos los nombres de host que han sido identificados durante la fuerza bruta de prefijos. Y adicionalmente identifica sistemas que pueden ser controlados por el mismo dominio, mediante búsquedas IP sobre otras direcciones dentro del bloque de clase C que ha sido identificado.



El archivo creado donde residen los resultados obtenidos por Fierce, puede ser visualizado utilizando un navegador como IceWeasel en Kali Linux.