# 3.1.9 Práctica de laboratorio - Búsquedas de DNS

**Objetivos**

El reconocimiento pasivo es un método de recopilación de información en el que las herramientas no interactúan directamente con el dispositivo o la red de destino. En esta práctica de laboratorio, explorará herramientas comunes utilizadas para recopilar información sobre un objetivo a través del Sistema de nombres de dominio (DNS).

Utilice nslookup para obtener información de dominio y dirección IP.
Utilice el comando whois para encontrar información de registro adicional.
Compare el resultado de las herramientas Nslookup y Dig.
Realizar búsquedas DNS inversas.

**Trasfondo / Escenario**

Antes de comenzar cualquier prueba de penetración u otro compromiso de piratería ética, debe obtener de manera encubierta tanta información sobre la organización objetivo. Existe una gran cantidad de información que se puede obtener a partir de los datos de registro de dominios disponibles públicamente. En esta práctica de laboratorio, investigará el resultado de los comandos nslookup, whois y dig.

**Instrucciones**

Parte 1: Utilice nslookup para obtener información de dominio y dirección IP.

*Paso 1: Inicie sesión en Kali Linux y acceda al entorno de la terminal.*

Inicie sesión en el sistema Kali con el nombre de usuario kali y la contraseña kali. Se le presenta el escritorio Kali.
Abra una ventana de terminal haciendo clic en el icono Terminal ubicado cerca de la parte superior de la pantalla.

*Paso 2: Investigación de las capacidades de nslookup*

Nslookup es una herramienta de línea de comandos disponible en Linux y Windows. Su uso básico es convertir un nombre de dominio en una dirección IP. Nslookup tiene otra funcionalidad que puede proporcionar información adicional.

Acceda a las páginas del manual de nslookup con el comando man :

```
┌──(kali㉿Kali)-[~]
└─$ man nslookup
```

Para revisar las páginas del manual, presione la barra espaciadora para avanzar las páginas. Cuando haya terminado de revisar las páginas del manual, presione q para salir y volver a la línea de comando.
¿Qué palabra clave set usaría para consultar el registro mx del servidor de correo dentro de un dominio?
Área de Respuesta

**nslookup -type=MX -debug cisco.com**

*Paso 3: Utilizar el comando nslookup*

Utilice el comando nslookup sin opciones para ingresar al modo interactivo. Para salir del modo interactivo en cualquier momento, escriba exit para volver al indicador de la CLI.
El indicador de la CLI cambia a > para indicar que ahora está en modo interactivo y puede ingresar los diversos comandos de nslookup. Ingrese el nombre de dominio cisco.com para resolver el nombre de dominio en una dirección IP. De manera predeterminada, el comando nslookup consulta los registros A y AAAA del destino.
> cisco.com
La salida del comando será similar a la que se muestra. El registro A contiene la dirección IPv4 asignada al dominio raíz y el registro AAAA contiene la dirección IPv6.

```
┌──(kali㉿Kali)-[~]
└─$ nslookup
> cisco.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   cisco.com
Address: 72.163.4.185
Name:   cisco.com
Address: 2001:420:1101:1::185
>
```

Para encontrar los servidores de nombres de dominio configurados para cisco.com, use el comando set type para cambiar el tipo de consulta a “ns” para devolver la información del servidor de nombres.
> set type=ns
> cisco.com
La salida del comando debe ser similar a la que se muestra a continuación. Los servidores se enumeran por nombre de dominio completo y, además, como servidores autorizados para direcciones IPv4 e IPv6.

```
> set type=ns
> cisco.com
;; communications error to 192.168.1.1#53: timed out
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
cisco.com       nameserver = ns1.cisco.com.
cisco.com       nameserver = ns3.cisco.com.
cisco.com       nameserver = ns2.cisco.com.

Authoritative answers can be found from:
```

ns2.cisco.com  internet address = 64.102.255.44
<output omitted>
¿Cuáles son las direcciones IPv4 e IPv6 del servidor DNS principal (ns1)?

Área de Respuesta

**Server Name: NS1.CISCO.COM**
**IP Address: 72.163.5.201**
**IP Address: 2001:420:1101:6:0:0:0:A**

Introduzca exit para salir del modo interactivo y volver al indicador de la CLI.

*Paso 4: Cambie el servidor utilizado para realizar las búsquedas.*

Ocasionalmente, es conveniente utilizar un servidor DNS diferente para realizar búsquedas. Esto puede ser necesario si el servidor DNS local no puede resolver una dirección o resuelve el nombre de host en una dirección privada interna y necesita obtener la dirección accesible de Internet del host.

En esta consulta, use la sintaxis del comando de una línea nslookup para cambiar el servidor y buscar skillsforall.com. La sintaxis del comando es nslookup [nombre de host] [IP del servidor].

```
┌──(kali㉿Kali)-[~]
└─$ nslookup skillsforall.com 8.8.8.8
```

En el modo interactivo, se cambia el servidor con la palabra clave server.

```
┌──(kali㉿Kali)-[~]
└─$ nslookup
> server 8.8.8.8
> skillsforall.com
```

El tipo de consulta any puede recuperar gran parte o toda la información contenida en el registro DNS para un nombre de host. A menudo, los registros de text (texto) que pueden proporcionar detalles adicionales sobre el dominio se encuentran en los registros de DNS. Con el servidor DNS de Google 8.8.8.8, busque los registros DNS de skillsforall.com.

```
┌──(kali㉿Kali)-[~]
└─$ nslookup
> server 8.8.8.8
> set type=any
> skillsforall.com
```

El resultado debería ser similar a este ejemplo:

```
┌──(kali㉿Kali)-[~]
└─$ nslookup
> server 8.8.8.8
Default server: 8.8.8.8
```

```
Address: 8.8.8.8#53
> set type=any
> skillsforall.com
;; Connection to 8.8.8.8#53(8.8.8.8) for skillsforall.com failed: timed out.
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   skillsforall.com
Address: 13.225.142.127
Name:   skillsforall.com
Address: 13.225.142.7
Name:   skillsforall.com
Address: 13.225.142.73
Name:   skillsforall.com
Address: 13.225.142.9
skillsforall.com        nameserver = ns-1130.awsdns-13.org.
skillsforall.com        nameserver = ns-1652.awsdns-14.co.uk.
skillsforall.com        nameserver = ns-489.awsdns-61.com.
skillsforall.com        nameserver = ns-588.awsdns-09.net.
skillsforall.com
        origin = ns-1130.awsdns-13.org
        mail addr = awsdns-hostmaster.amazon.com
        serial = 1
        refresh = 7200
        retry = 900
        expire = 1209600
        minimum = 86400
skillsforall.com        mail exchanger = 10 inbound-smtp.us-east-1.amazonaws.com.
skillsforall.com        text = "d1g1l9y74sxj8m.cloudfront.net"
skillsforall.com        text = "facebook-domain-verification=8cg08gu4eikp0d2d1quqhjwh5ti1vv"
skillsforall.com        text = "google-site-
verification=Q5NIWRygJYTSLxuHReNKw1kvgC8IXKTOyPf5zITDv40"
skillsforall.com        text =
"identrust_validate=tadDBgWwQAKpw6QCCQDCagqsZgxHELybnPOCQHNU+rsV"
```

¿Qué tipos de registro se muestran en la salida del comando nslookup con el tipo establecido en any?

Área de Respuesta

**A, AAAA, ns, mx y text.**

*Parte 2: Usar la función Whois para obtener información del dominio*

La herramienta whois consulta la información de registro de dominio, en lugar de los registros del servidor DNS. Es otra forma de reconocimiento pasivo que puede identificar dónde está registrado el dominio, información de contacto técnica y administrativa y ubicaciones físicas. Tenga en cuenta que la información contenida en los registros de dominio se puede configurar como privada y, a menudo, la información de contacto es la del servicio de alojamiento, en lugar de la organización en sí.

*Paso 1: Compare el resultado de whois de varias organizaciones.*

La herramienta whois está disponible desde el indicador CLI en Kali Linux. Utilice el comando whois para obtener información sobre cisco.com.

```
┌──(kali㉿Kali)-[~]
└─$ whois cisco.com
```

Ahora use el comando whois para obtener información sobre el dominio skillsforall.com.
¿Qué conclusión puede sacar sobre los dos dominios (cisco.com y skillsforall.com) en función del resultado de los comandos whois?
Área de Respuesta

**El dominio skillsforall.com no es un dominio independiente de una empresa externa, sino un dominio registrado y administrado por Cisco Technology Inc.. Esto confirma que Skills for All es una plataforma oficial de Cisco y no un sitio de terceros. Además, el uso de AWS para el hosting sugiere que Cisco ha optado por una solución en la nube para este proyecto en lugar de su infraestructura interna.**

*Paso 2: Utilice whois para determinar la información de registro de la dirección IP.*

La herramienta Whois también se puede utilizar para recopilar información sobre los rangos de direcciones IP asignados a una organización. En la parte anterior de esta práctica de laboratorio, descubrimos las direcciones IP asignadas a varios nombres de host de servidores DNS de dominio. Ahora puede usar esa información de dirección para obtener detalles adicionales sobre los rangos de direcciones IP externas que se asignan a esas organizaciones.

Revise el resultado que obtuvo al usar nslookup para obtener las direcciones IP del servidor DNS para cisco.com. Registre las direcciones IP de los servidores DNS de Cisco.
Use la herramienta Whois para encontrar qué rangos de direcciones IP están asignados a Cisco y se utilizan en las redes que alojan sus servidores DNS. En el momento de esta práctica de laboratorio, ns1.cisco.com se resolvía con la dirección IP 72.163.5.201; sin embargo, esto puede variar. Cuando se le solicite, ingrese whois 72.163.5.201.

```
┌──(kali㉿Kali)-[~]
└─$ whois 72.163.5.201

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
```

#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#

#

NetRange: 72.163.0.0 - 72.163.255.255
CIDR: 72.163.0.0/16
NetName: CISCO-GEN-7
NetHandle: NET-72-163-0-0-1
Parent: NET72 (NET-72-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS109
Organization: Cisco Systems, Inc. (CISCOS-2)
RegDate: 2006-10-24
Updated: 2022-06-09
Ref: https://rdap.arin.net/registry/ip/72.163.0.0

OrgName: Cisco Systems, Inc.
OrgId: CISCOS-2
Address: 170 West Tasman Drive
City: San Jose
StateProv: CA
PostalCode: 95134
Country: US
RegDate: 1986-02-05
Updated: 2021-10-27
Ref: https://rdap.arin.net/registry/entity/CISCOS-2

OrgTechHandle: CAMT-ARIN
OrgTechName: Cisco address management team
<output omitted>
¿Cuál es el rango de direcciones IP para las direcciones IPv4 asignadas a Cisco? El servidor ns1.cisco.com se direcciona dentro de este bloque.
Área de Respuesta

**CIDR: 72.163.0.0/16**

Debido a que las organizaciones pueden usar las mismas redes IP para otros servidores externos, conocer los rangos de direcciones es valioso para determinar a qué redes apuntar durante una prueba de penetración. Utilice la herramienta whois para obtener las asignaciones de direcciones IP para las redes IP donde se encuentran los otros servidores DNS de Cisco.

**Parte 3: Comparar el resultado de las funciones Nslookup y Dig**

*Paso 1: Utilice Linux Dig para consultar servidores DNS.*

Dig es una función de Linux que realiza consultas al DNS. El formato de una consulta Dig es similar a la de Nslookup. Para resolver el nombre de host cisco.com en una dirección IP, utilice la sintaxis dig [nombre del host].

```
┌──(kali㉿Kali)-[~]
└─$ dig cisco.com
```

¿Cuál es la diferencia entre los tipos de registro predeterminados consultados por Dig y los consultados por Nslookup?

Área de Respuesta

💡 **Conclusión:**

**nslookup consulta automáticamente A y AAAA.**

**dig consulta solo A, a menos que se especifique otro tipo de registro.**

**dig ofrece más detalles sobre la consulta (tiempos, cabeceras DNS, EDNS, etc.).**

Para obtener la dirección IPv6 de cisco.com, es necesario agregar un tipo a la estructura de comando. La sintaxis para indicar a Dig que consulte un tipo de registro específico es dig [hostname] [record type].

```
┌──(kali㉿Kali)-[~]
└─$ dig cisco.com AAAA
```

Paso 2: Utilice Dig para obtener información adicional.

En la primera parte de esta práctica de laboratorio, se utilizó nslookup para obtener los servidores DNS para cisco.com. Utilice el servidor DNS de Google 8.8.8.8 para consultar los registros del servidor DNS. La sintaxis para utilizar un comando dig para realizar una consulta con un servidor DNS diferente es dig [nombre de host] @ [IP del servidor DNS] [tipo]. En la línea de comandos, ingrese dig cisco.com 8.8.8.8 ns.

```
┌──(kali㉿Kali)-[~]
└─$ dig cisco.com 8.8.8.8 ns

; <<>> DiG 9.18.8-1-Debian <<>> cisco.com @8.8.8.8 ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62945
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;cisco.com.                     IN      NS

;; ANSWER SECTION:
cisco.com.              1493    IN      NS      ns3.cisco.com.
cisco.com.              1493    IN      NS      ns1.cisco.com.
cisco.com.              1493    IN      NS      ns2.cisco.com.

;; Query time: 83 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Fri Mar 03 21:15:13 UTC 2023
;; MSG SIZE  rcvd: 92
```

<output omitted>

Anteriormente, nslookup se usaba con la opción set type=any para encontrar información adicional sobre el nombre de host de skillsforall.com. El tipo de registro any también se puede consultar mediante Dig.

```
┌──(kali㉿Kali)-[~]
└─$ dig skillsforall.com any
```

Compare la salida de la función Dig con la salida de Nslookup para el tipo de registro any. ¿Qué salida es más fácil de leer para obtener los valores contenidos en los diversos tipos de registros?

Área de Respuesta

**¿Cuál es más fácil de leer?**
**nslookup es más fácil de leer si solo te interesa obtener rápidamente las direcciones IP (tanto IPv4 como IPv6) sin mucha información adicional.**

**dig es más adecuado si necesitas detalles como los tiempos de respuesta, información sobre el servidor DNS, y otras configuraciones, pero es menos amigable si solo necesitas una salida simple.**

Parte 4: Realizar búsquedas de DNS inversas

Paso 1: Utilizar Dig para realizar búsquedas de rDNS

Ahora que puede realizar búsquedas de DNS y usar Whois para determinar rangos de direcciones IP, use Dig para buscar nombres de host adicionales. Las búsquedas de DNS inverso (rDNS) utilizan la dirección IP para consultar los nombres de host de los servicios que se resuelven en esa dirección.

Introduzca el comando dig con la opción -x para recuperar el nombre de host y el tipo de registro del servidor DNS ns1.cisco.com (72.163.5.201).

```
┌──(kali㉿Kali)-[~]
└─$ dig -x 72.163.5.201
```

¿Qué tipo de registro se devuelve con el nombre de host?

Área de Respuesta

**41.137.120.34.bc.googleusercontent.com.**

Utilice el comando dig -x para consultar otra dirección IP en la misma subred.

```
┌──(kali㉿Kali)-[~]
└─$ dig -x 72.163.1.1
```

Examine la salida devuelta por el comando dig. ¿Qué tipo de dispositivo cree que tiene asignada la dirección 72.163.1.1?

Área de Respuesta

**Conclusión:**
**La IP 34.120.1.1 está asociada a un servidor o dispositivo virtual alojado en Google Cloud, y no a un dispositivo físico directamente. Es posible que esté siendo utilizada por uno de los clientes de Google Cloud para ejecutar servicios en línea, aplicaciones o servidores en la infraestructura de Google**.

Paso 2: Usar la utilidad de host para realizar búsquedas de rDNS

La utilidad Host es una función en Linux que realiza búsquedas para convertir direcciones IP en nombres de host. Utilice esta utilidad para buscar otro host en la red 72.163.0.0/16.

La sintaxis del comando host es host [dirección IP o nombre de host]

```
┌──(kali㉿Kali)-[~]
└─$ host 72.163.10.1
```

El host también se puede utilizar para realizar una búsqueda rápida de direcciones IP para un nombre de host conocido.

```
┌──(kali㉿Kali)-[~]
└─$ host hsrp-72-163-10-1.cisco.com
```

¿En qué se diferencia la salida del comando host de Dig o Nslookup al consultar una dirección IP asignada a un host conocido?

Área de Respuesta

**host es más sencillo y se utiliza para obtener rápidamente el nombre asociado a una IP.**

**dig es más avanzado, mostrando una salida detallada de la consulta y los resultados.**

**nslookup proporciona información técnica de manera intermedia, pero es menos detallado que dig.**

Las URL a menudo contienen alias para el nombre de host del servidor que aloja el sitio web. La salida del comando host puede enumerar los servidores que responden a esa URL.

```
┌──(kali㉿Kali)-[~]
└─$ host hsrp-72-163-10-1.cisco.com
```

La información sobre los alias es útil al intentar determinar dónde se encuentra el sitio web o el servicio real.

Paso 3: Utilice nslookup para realizar búsquedas de rDNS

Nslookup se usa principalmente para realizar búsquedas de direcciones IP para nombres de host conocidos. También se puede utilizar para realizar búsquedas de rDNS para devolver un nombre de host asignado a una dirección IP conocida.

Utilice Nslookup para encontrar nombres de host asociados con una dirección IP.

En el modo no interactivo, la sintaxis para realizar una consulta rDNS es nslookup [dirección IP].

```
┌──(kali㉿Kali)-[~]
└─$ nslookup 72.163.5.201
```

Para usar el modo interactivo, ingrese nslookup sin opciones. En el indicador >, introduzca la dirección IP de destino.

```
┌──(kali㉿Kali)-[~]
└─$ nslookup
> 72.163.5.201
```

Reflexión
En esta práctica de laboratorio, utilizó nslookup, dig y host para obtener información de los archivos de zona DNS. ¿Qué herramienta usaría para comenzar un esfuerzo de reconocimiento pasivo contra un dominio objetivo? ¿Por qué?

Área de Respuesta

**Usa dig para un esfuerzo de reconocimiento pasivo porque:**

**Proporciona detalles completos sobre los registros DNS.**

**Es flexible y permite realizar consultas avanzadas de registros específicos.**

**Es fiable y tiene una salida clara y detallada.**

**Con dig, puedes obtener toda la información necesaria para mapear la infraestructura de red y los servicios asociados a un dominio sin causar alertas o tener interacción directa con el sistema objetivo, lo cual es esencial en el reconocimiento pasivo.**