ETHICAL HACKING V2
LAB SERIES

Lab 01: DNS Footprinting

Document Version: 2020-08-24

Material in this Lab Aligns to the Following	
Books/Certifications	**Chapters/Modules/Objectives**
All-In-One CEH Chapters ISBN-13: 978-1260454550	2: Reconnaissance: Information Gathering for the Ethical Hacker
EC-Council CEH v10 Domain Modules	2: Footprinting and Reconnaissance
CompTIA Pentest+ Objectives	2.1: Given a scenario, conduct information gathering using appropriate techniques 4.2: Compare and contrast various use cases of tools
CompTIA All-In-One PenTest+ Chapters ISBN-13: 978-1260135947	2: Getting to Know Your Targets 3: Network Scanning and Enumeration 4: Vulnerability Scanning and Analysis

Contents

Introduction

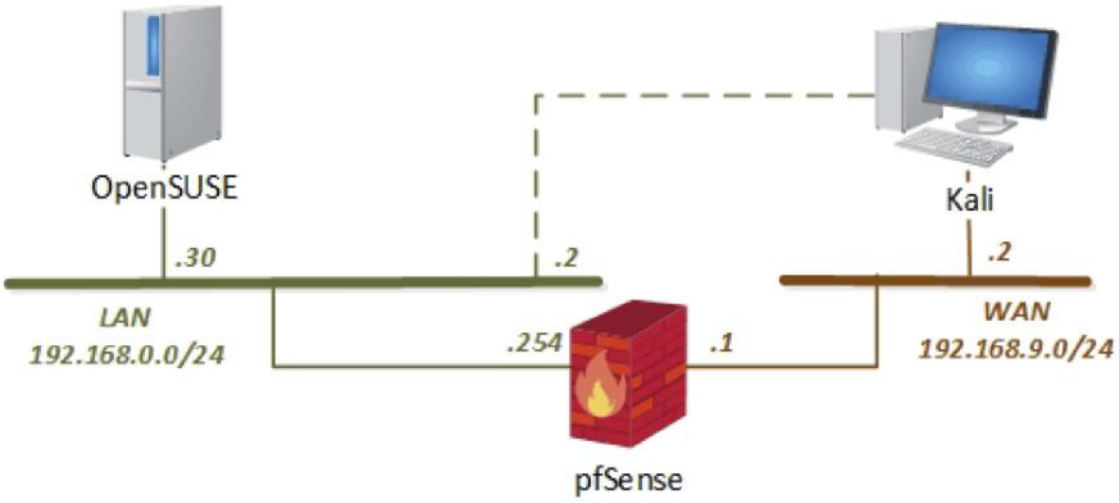
This lab introduces *nslookup* and *dig* which are two commonly used DNS footprinting tools.

Objective

In this lab, you will be conducting ethical hacking practices using various tools. You will be performing the following tasks:

1. Footprinting with nslookup
2. Comparing nslookup with dig

Pod Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Kali Linux	192.168.9.2 192.168.0.2	root	toor
pfSense	192.168.0.254 192.168.68.254 192.168.9.1	admin	pfsense
OpenSUSE	192.168.0.30	osboxes	osboxes.org

1 Footprinting using nslookup

The *nslookup* tool is available on both Windows and Linux to query DNS records.

1. Click on the **Kali** tab.
2. Click within the console window and press **Enter** to display the login prompt.
3. Enter **`root`** as the *username*. Press **Tab**.
4. Enter **`toor`** as the *password*. Click **Log In**.
5. Open a new terminal by clicking on the **Terminal** icon located at the top of the page, if the terminal is not already opened.
6. Open and review *nslookup's* manual by typing the command below, followed by pressing **Enter**.

```
man nslookup
```

nslookup has many commands. Review the man pages to get familiar with them. Press the Spacebar to go to the next page or press Enter to go to the next line.

7. Once finished reviewing the man page, press the **Q** character to quit and bring the shell prompt back.

8. In the *Terminal* window, initiate *nslookup* interactive mode by typing the following command, then press **Enter.**

```
nslookup
```

9. At the prompt, we can type **`server`** to see our current lookup server:

```
server
```

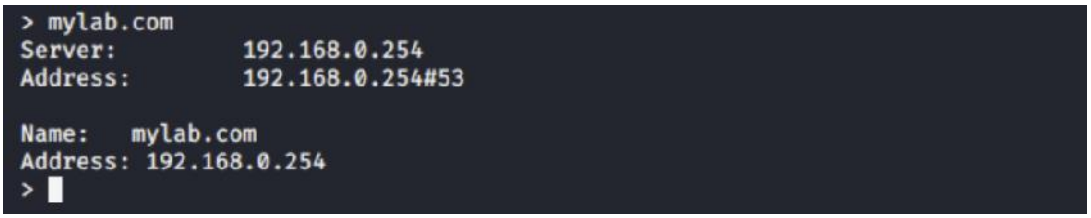
Notice the default server listed is the pfSense firewall from the topology.

10. For this lab environment, the DNS server we want to query is only listening on IP address 192.168.0.254. Change the default server by typing the following command and pressing **Enter.**

```
server 192.168.0.254
```

11. In the lab environment, we have a domain called **mylab.com,** and we want to see what the root domain resolves to. To do a domain lookup, type the following command and press **Enter**.

```
mylab.com
```



12. DNS has multiple record types. Below is a table of common types:

Record Type	Brief Description	Explanation
A	Host Address for IPv4	This is generally an IPv4 address.
AAAA	Host Address for IPv6	This is generally an IPv6 address.
CNAME	Canonical Name	Maps an alias to the canonical name. Often used to point multiple systems to one IP without assigning an A record to each hostname. The DNS lookup will continue by retrying the lookup with the new name.
MX	Mail Exchanger	Maps a domain name to a list of message transfer agents.
NS	Nameserver	Delegates a DNZ zone to use the given authoritative name servers.
PTR	Pointer	Points to a canonical name. Unlike CNAME, the DNS lookup process stops, and just the name is returned.
SOA	Start of Authority	Specifies authoritative information about a DNS zone.
SRV	Service Location	Generalized service location record.
TXT	Text	Originally for arbitrary human-readable text in a DNS record, it is now used for several other machine-readable data types.

To explore these, we use the *set* command. Type the following command to set the type to *ns* (nameserver) and press **Enter.**

```
set type=ns
```

13. Once the type has been set, type in the following command to check the domain again and press **Enter.**

```
mylab.com
```



```
> set type=ns
> mylab.com
Server:         192.168.0.254
Address:        192.168.0.254#53

mylab.com       nameserver = 192.168.0.254.
> 
```

The output here shows the nameserver for the mylab.com domain. In this case, it is 192.168.0.254. If doing this with a public domain, the server would typically return the nameserver different than the server you are using for lookups, unless that DNS server is hosting that domain.

14. By default, *nslookup* returns *a* records. Here we will look up the *a* record for the host **opensuse.mylab.com** by typing the following and pressing **Enter** after each line**.**

```
set type=a
opensuse.mylab.com
```

```
> set type=a
> opensuse.mylab.com
Server:         192.168.0.254
Address:        192.168.0.254#53

Name:   opensuse.mylab.com
Address: 192.168.0.30
> 
```

The output here shows us that the IP address for opensuse.mylab.com is 192.168.0.30.

15. Now try to return *mx* (mail servers) records for the domain. Type each command below, pressing **Enter** after each line:

```
set type=mx
mylab.com
```

```
> set type=mx
> mylab.com
Server:         192.168.0.254
Address:        192.168.0.254#53

** Can't find mylab.com: No answer
> 
```

Notice there is “no answer” from the DNS server. This DNS server is configured to not respond to all request types. There is, in fact, an *mx* record, which you will find later.

16. One lookup type not on the list is *any.* Instinctively, you may want to set the type to *any* and get everything back! Newer DNS servers do not return everything for the zone. While getting some good information, you will not see all the hosts or *a* records on that domain. Type each command below, pressing **Enter** after each line:

```
set type=any
mylab.com
```

17. In order to get to see EVERYTHING, you need to be able to access an *axfr* (transfer) record. Normally, these are not available. You can test this on the Kali machine by typing each command below, pressing **Enter** after each line:

```
set type=axfr
mylab.com
```

Notice this is not a "no answer" response from the DNS server, but rather a REFUSED response.

18. The OpenSUSE machine has been allowed to pull transfer records. Click on the **OpenSUSE** tab.
19. Enter **osboxes** as the *username*.
20. Enter **osboxes.org** as the *password*. Press **Enter.**
21. Click on the **Konsole** icon in the lower-right to launch a new terminal.

22. In the *Konsole* window, initiate *nslookup* by typing the following command, then press **Enter.**

```
nslookup
```

```
osboxes@osboxes:~> nslookup
> 
```

23. In order to get to see EVERYTHING, try again to access an *axfr* (transfer) record. Test this on the OpenSUSE machine by typing each command below, pressing **Enter** after each line:

```
set type=axfr
mylab.com
```

```
> set type=axfr
> mylab.com
Server:         192.168.0.254
Address:        192.168.0.254#53

mylab.com
        origin = 192.168.0.254
        mail addr = zonemaster.mylab.com
        serial = 2576776945
        refresh = 86400
        retry = 7200
        expire = 2419200
        minimum = 3600
mylab.com       nameserver = 192.168.0.254.
Name:   mylab.com
Address: 192.168.0.254
linux.mylab.com canonical name = opensuse.mylab.com.
mail.mylab.com  mail exchanger = 10 mail.mylab.com.
ns1.mylab.com   nameserver = 192.168.0.254.mylab.com.
Name:   opensuse.mylab.com
Address: 192.168.0.30
Name:   pfsense.mylab.com
Address: 192.168.0.254
Name:   seconion.mylab.com
Address: 192.168.0.100
SEE\032MY\032TXT\032RECORD.mylab.com     text = "mytext"
windows.mylab.com       canonical name = winos.mylab.com.
Name:   winos.mylab.com
Address: 192.168.0.20
mylab.com
        origin = 192.168.0.254
        mail addr = zonemaster.mylab.com
        serial = 2576776945
        refresh = 86400
        retry = 7200
        expire = 2419200
        minimum = 3600
> 
```

In the output, you will see every record on the domain, including A, SOA, CNAME, TXT, MX, and NS records.

24. To exit from the *nslookup* utility, type the following command and press **Enter**:

```
exit
```

```
osboxes@osboxes:~> 
```


2 Comparing nslookup with dig

1. Dig is a similar tool used for viewing DNS information. Type the following command into the OpenSUSE terminal to see the *nslookup* equivalent of a nameserver lookup and press **Enter:**

```
dig @192.168.0.254 mylab.com ns
```

Command	Explanation
dig	The program you are using.
@192.168.0.254	The server to lookup from.
mylab.com	The name you are looking for.
ns	The type of record.

The equivalent one-line command for *nslookup* is:

nslookup -type=ns -debug mylab.com 192.168.0.254

Notice we had to enable debug mode to see similar output. Dig is not installed on Windows systems by default and must be downloaded.

2. You may now end your reservation.

