Laboratory Exercise 4-4 – Advanced Enumeration

1. Overview

For this lesson, students will use the Cyber Range: Kali Linux with Metasploitable3 Environment to complete enumeration with DNSmap, Nslookup, Enum4Linux, and DIG.

2. Resources required

This exercise requires the latest Kali Linux with Metasploitable3 Environment running in the Cyber Range.

3. Initial Setup

For this exercise, you will log in to your Cyber Range account and select the Kali Linux with Metasploitable3 Environment, then click "start" to start your environment and "join" to get to your Linux desktop login. Log in using these credentials:

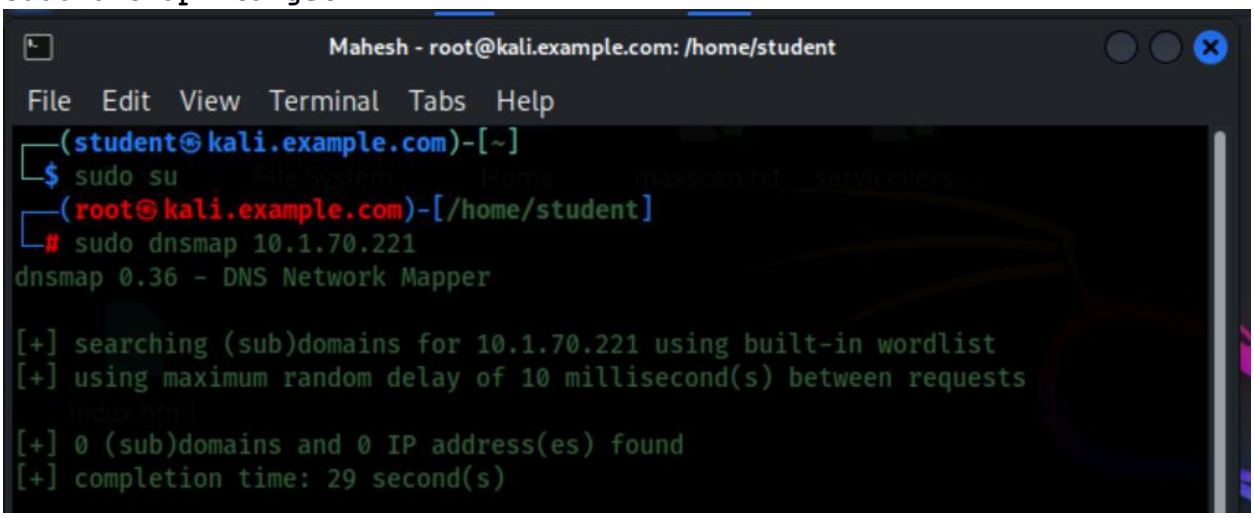
Username: **student**
Password: **student**

4. Tasks

Task 1: Using DNSmap to Enumerate DNS

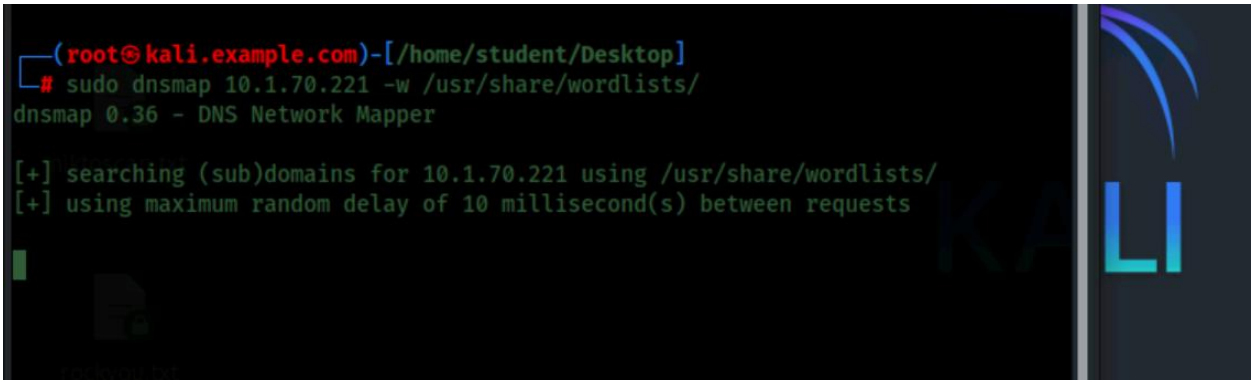
DNSmap is a very easy to use tool. The syntax is as follows:

```
sudo dnsmap <target>
```



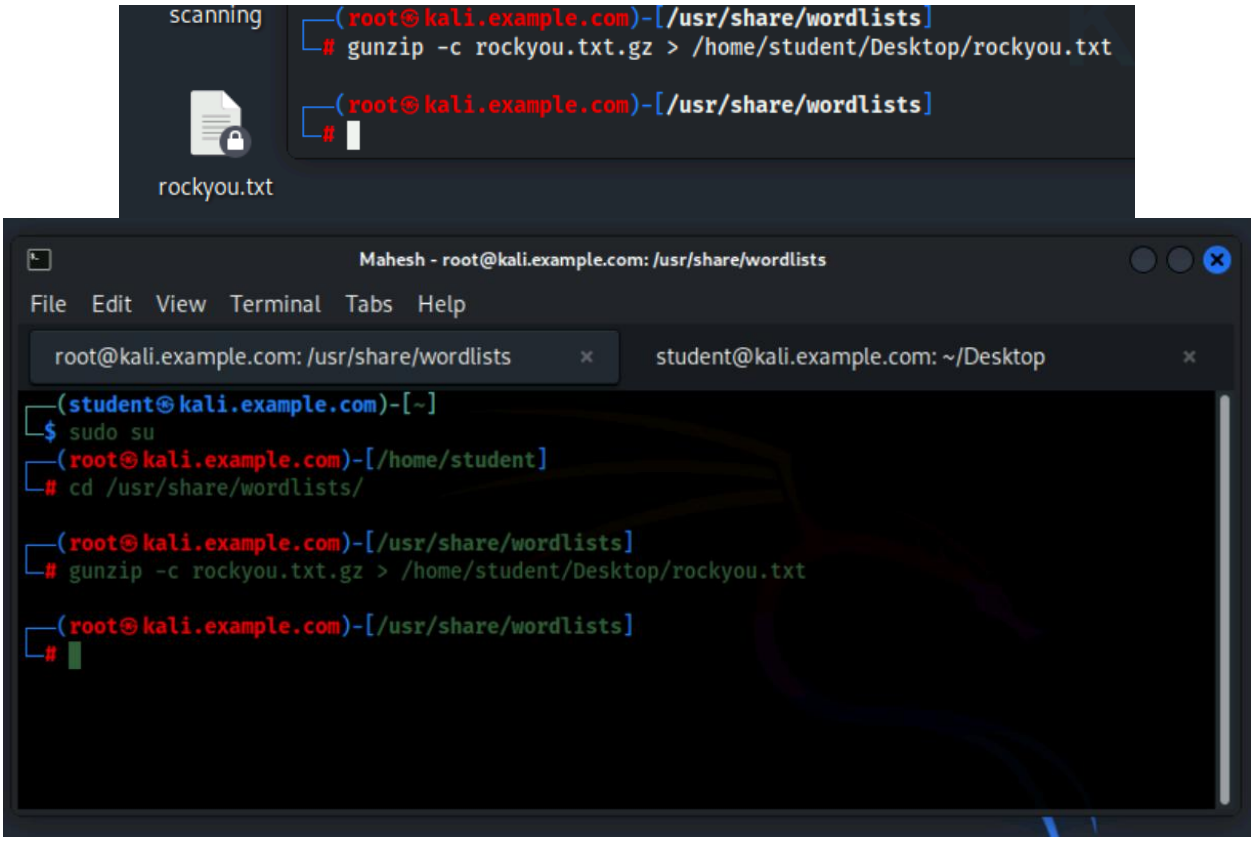
To brute force the DNS, use the following syntax:

```
sudo dnsmap <target> -w <path files>
```



For this task, we will attempt to enumerate our target2.example.com site. We will not be using a wordlist as this is out of scope; however, the rockyou.txt is a wordlist that can be used for a task like this. The wordlist is found at /usr/share/wordlists/. You will need to navigate to that directory and be root to see and extract the tar file. I have provided the syntax below for those who do not remember from previous courses. This will place the rockyou.txt on the student desktop.

- **`gunzip -c rockyou.txt.gz > /home/student/Desktop/rockyou.txt`**



Oftentimes, creating a custom wordlist is a probable solution as well. Keep in mind, that brute forcing a DNS can take days or even weeks.

Reminder** **Do NOT scan domains that you do not have permission to scan.**

Complete the following:

1. Scan tesla.com with DNSmap. Try both examples described above. Tesla has an open bug bounty program and allows scanning. The rockyou.txt file can be used. The program can be viewed at https://bugcrowd.com/teslav. The DNS brute force attempt with the rockyou.txt will take a long time. If there are no results in a reasonable amount of time, cancel the scan with CTRL+C.

   Type **`sudo dnsmap <target>`** where <target> is tesla.com. See the image below.

```
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# sudo dnsmap tesla.com
dnsmap 0.36 - DNS Network Mapper

[+] searching (sub)domains for tesla.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

accounts.tesla.com
IPv6 address #1: 2600:1408:ec00:282::700
IPv6 address #2: 2600:1408:ec00:283::700

accounts.tesla.com
IP address #1: 23.56.8.49

bi.tesla.com
IP address #1: 23.209.118.211

billing.tesla.com
IPv6 address #1: 2600:1408:ec00:981::700

billing.tesla.com
IP address #1: 23.39.184.66

cx.tesla.com
```

Mahesh - root@kali.example.com: /usr/share/wordlists

File Edit View Terminal Tabs Help

root@kali.example.com: /usr/share/wordlists | student@kali.example.com: ~/Desktop

```
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# sudo dnsmap tesla.com
dnsmap 0.36 - DNS Network Mapper

[+] searching (sub)domains for tesla.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

accounts.tesla.com
IPv6 address #1: 2600:1408:20:a92::700
IPv6 address #2: 2600:1408:20:abf::700

accounts.tesla.com
IP address #1: 23.220.128.92

bi.tesla.com
IP address #1: 23.209.118.211

billing.tesla.com
IPv6 address #1: 2600:1408:ec00:998::700
IPv6 address #2: 2600:1408:ec00:98c::700

billing.tesla.com
IP address #1: 23.220.132.93

cx.tesla.com
IPv6 address #1: 2600:1408:ec00:998::700
IPv6 address #2: 2600:1408:ec00:98c::700

cx.tesla.com
IP address #1: 23.220.132.93
```

```
Mahesh - root@kali.example.com: /usr/share/wordlists
File  Edit  View  Terminal  Tabs  Help
root@kali.example.com: /usr/share/wor...   student@kali.example.com: ~/Desktop

mobile.tesla.com
IPv6 address #1: 2600:1408:ec00:998::700
IPv6 address #2: 2600:1408:ec00:98c::700

mobile.tesla.com
IP address #1: 23.55.200.89

partners.tesla.com
IPv6 address #1: 2600:1408:ec00:998::700
IPv6 address #2: 2600:1408:ec00:98c::700

partners.tesla.com
IP address #1: 23.220.132.93

shop.tesla.com
IPv6 address #1: 2600:1408:ec00:98c::700
IPv6 address #2: 2600:1408:ec00:998::700

shop.tesla.com
IP address #1: 23.55.200.89

vpn1.tesla.com
IP address #1: 8.45.124.215

vpn2.tesla.com
IP address #1: 8.47.24.215

vpn3.tesla.com
IP address #1: 8.21.14.215

www.tesla.com
IPv6 address #1: 2600:1408:ec00:98c::700
IPv6 address #2: 2600:1408:ec00:998::700

www.tesla.com
IP address #1: 23.220.132.93

[+] 22 (sub)domains and 30 IP address(es) found
[+] completion time: 25 second(s)

┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─#
```

Now, type **`sudo dnsmap tesla.com -w /home/student/Desktop/rockyou.txt`** and hit enter. BE PATIENT: This will take some time. You can CTRL+C after some time; the main point is to see what kind of information this command will provide you as the pentester. See the image below.

```
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# sudo dnsmap tesla.com -w /home/student/Desktop/rockyou.txt
dnsmap 0.36 - DNS Network Mapper

[+] searching (sub)domains for tesla.com using /home/student/Desktop/rockyou.txt
[+] using maximum random delay of 10 millisecond(s) between requests

ranger.tesla.com
IPv6 address #1: 2600:1408:ec00:98c::700
IPv6 address #2: 2600:1408:ec00:981::700

ranger.tesla.com
IP address #1: 23.196.32.132

mobile.tesla.com
IPv6 address #1: 2600:1408:ec00:981::700
IPv6 address #2: 2600:1408:ec00:98c::700

mobile.tesla.com
IP address #1: 23.39.184.66
```

Mahesh - root@kali.example.com: /usr/share/wordlists

File Edit View Terminal Tabs Help

root@kali.example.com: /usr/share/wor... | student@kali.example.com: ~/Desktop

```
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# sudo dnsmap tesla.com -w /home/student/Desktop/rockyou.txt
dnsmap 0.36 - DNS Network Mapper

[+] searching (sub)domains for tesla.com using /home/student/Desktop/rockyou.txt
[+] using maximum random delay of 10 millisecond(s) between requests

ranger.tesla.com
IPv6 address #1: 2600:1408:ec00:98c::700
IPv6 address #2: 2600:1408:ec00:998::700

ranger.tesla.com
IP address #1: 23.55.200.89

mobile.tesla.com
IPv6 address #1: 2600:1408:ec00:998::700
IPv6 address #2: 2600:1408:ec00:98c::700

mobile.tesla.com
IP address #1: 23.220.132.93

kronos.tesla.com
IPv6 address #1: 2600:1408:ec00:998::700
IPv6 address #2: 2600:1408:ec00:98c::700

kronos.tesla.com
IP address #1: 23.220.132.93

inside.tesla.com
IPv6 address #1: 2600:1408:ec00:98c::700
IPv6 address #2: 2600:1408:ec00:998::700

inside.tesla.com
IP address #1: 23.220.132.93

marketing.tesla.com
IP address #1: 13.111.47.196

static.tesla.com
IPv6 address #1: 2600:1408:ec00:998::700
```

```
static.tesla.com
IP address #1: 23.45.148.67

profile.tesla.com
IPv6 address #1: 2600:1408:ec00:998::700
IPv6 address #2: 2600:1408:ec00:98c::700

profile.tesla.com
IP address #1: 23.55.200.89

service.tesla.com
IPv6 address #1: 2600:1408:ec00:998::700
IPv6 address #2: 2600:1408:ec00:98c::700

service.tesla.com
IP address #1: 23.220.132.93

track.tesla.com
IPv6 address #1: 2600:1408:ec00:998::700
IPv6 address #2: 2600:1408:ec00:98c::700

track.tesla.com
IP address #1: 23.220.132.93

hawkeye.tesla.com
IP address #1: 199.43.255.25
```

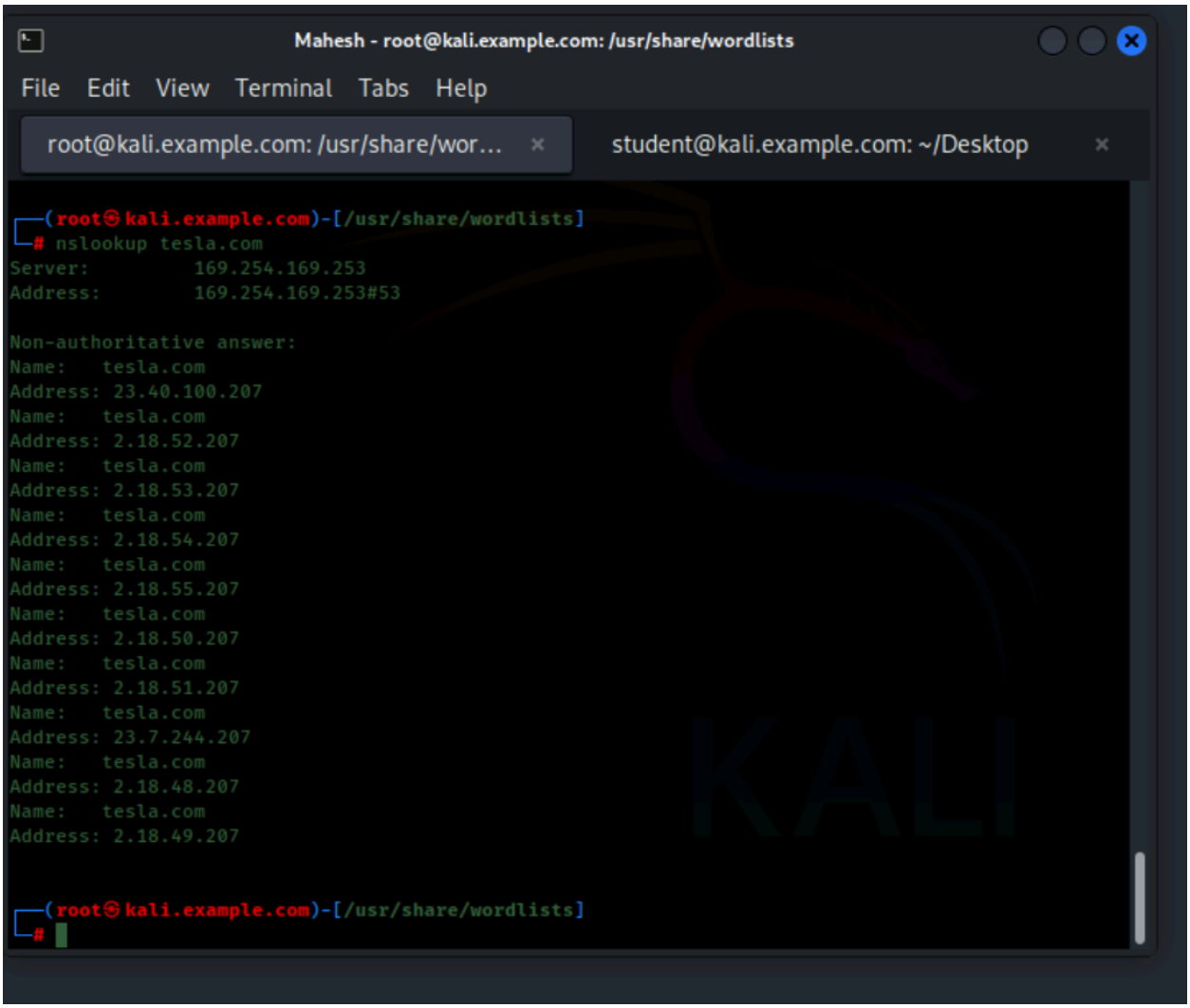
Task 2: Using Nslookup to perform DNS enumeration

Query tesla.com Domain Name Server (DNS) with the following command:

```
nslookup tesla.com
```

```
└# nslookup tesla.com
Server:         169.254.169.253
Address:        169.254.169.253#53

Non-authoritative answer:
Name:   tesla.com
Address: 2.18.55.207
Name:   tesla.com
Address: 2.18.50.207
Name:   tesla.com
Address: 2.18.51.207
Name:   tesla.com
Address: 23.7.244.207
Name:   tesla.com
Address: 2.18.48.207
Name:   tesla.com
Address: 2.18.49.207
Name:   tesla.com
Address: 23.40.100.207
Name:   tesla.com
Address: 2.18.52.207
Name:   tesla.com
Address: 2.18.53.207
Name:   tesla.com
```



Query for name server records with the following command:

```
nslookup -type=ns tesla.com
```

```
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# nslookup -type=ns tesla.com
Server:         169.254.169.253
Address:        169.254.169.253#53

Non-authoritative answer:
tesla.com       nameserver = a10-67.akam.net.
tesla.com       nameserver = a9-67.akam.net.
tesla.com       nameserver = a12-64.akam.net.
tesla.com       nameserver = edns69.ultradns.com.
tesla.com       nameserver = a1-12.akam.net.
tesla.com       nameserver = a28-65.akam.net.
tesla.com       nameserver = a7-66.akam.net.

Authoritative answers can be found from:
```

```
Mahesh - root@kali.example.com: /usr/share/wordlists
File  Edit  View  Terminal  Tabs  Help
root@kali.example.com: /usr/share/wor...   student@kali.example.com: ~/Desktop
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# nslookup -type=ns tesla.com
Server:         169.254.169.253
Address:        169.254.169.253#53

Non-authoritative answer:
tesla.com       nameserver = a9-67.akam.net.
tesla.com       nameserver = edns69.ultradns.com.
tesla.com       nameserver = a12-64.akam.net.
tesla.com       nameserver = a28-65.akam.net.
tesla.com       nameserver = a1-12.akam.net.
tesla.com       nameserver = a10-67.akam.net.
tesla.com       nameserver = a7-66.akam.net.

Authoritative answers can be found from:


┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─#
```

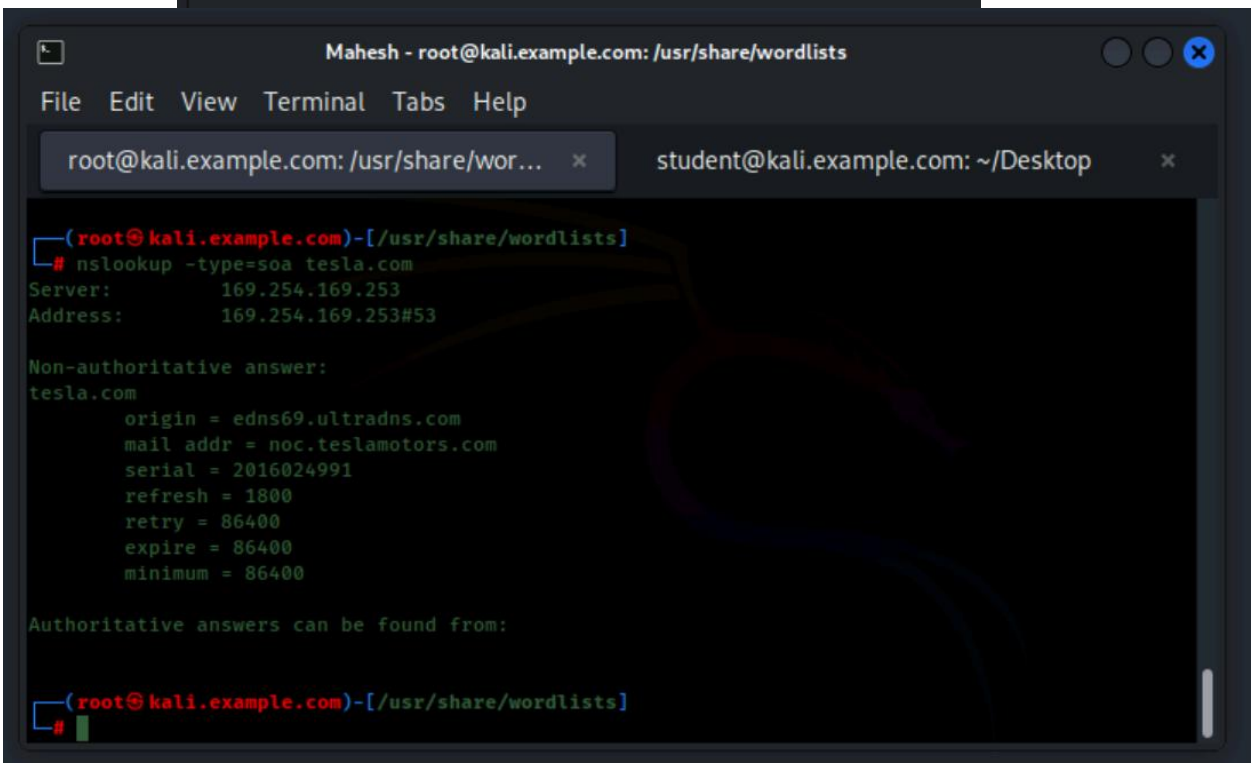
Query for start of authority (SOA) records with the following command:

```
nslookup -type=soa tesla.com
```

```
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# nslookup -type=soa tesla.com
Server:         169.254.169.253
Address:        169.254.169.253#53

Non-authoritative answer:
tesla.com
        origin = edns69.ultradns.com
        mail addr = noc.teslamotors.com
        serial = 2016024844
        refresh = 1800
        retry = 86400
        expire = 86400
        minimum = 86400

Authoritative answers can be found from:
```



Query for specific ports with the following command:

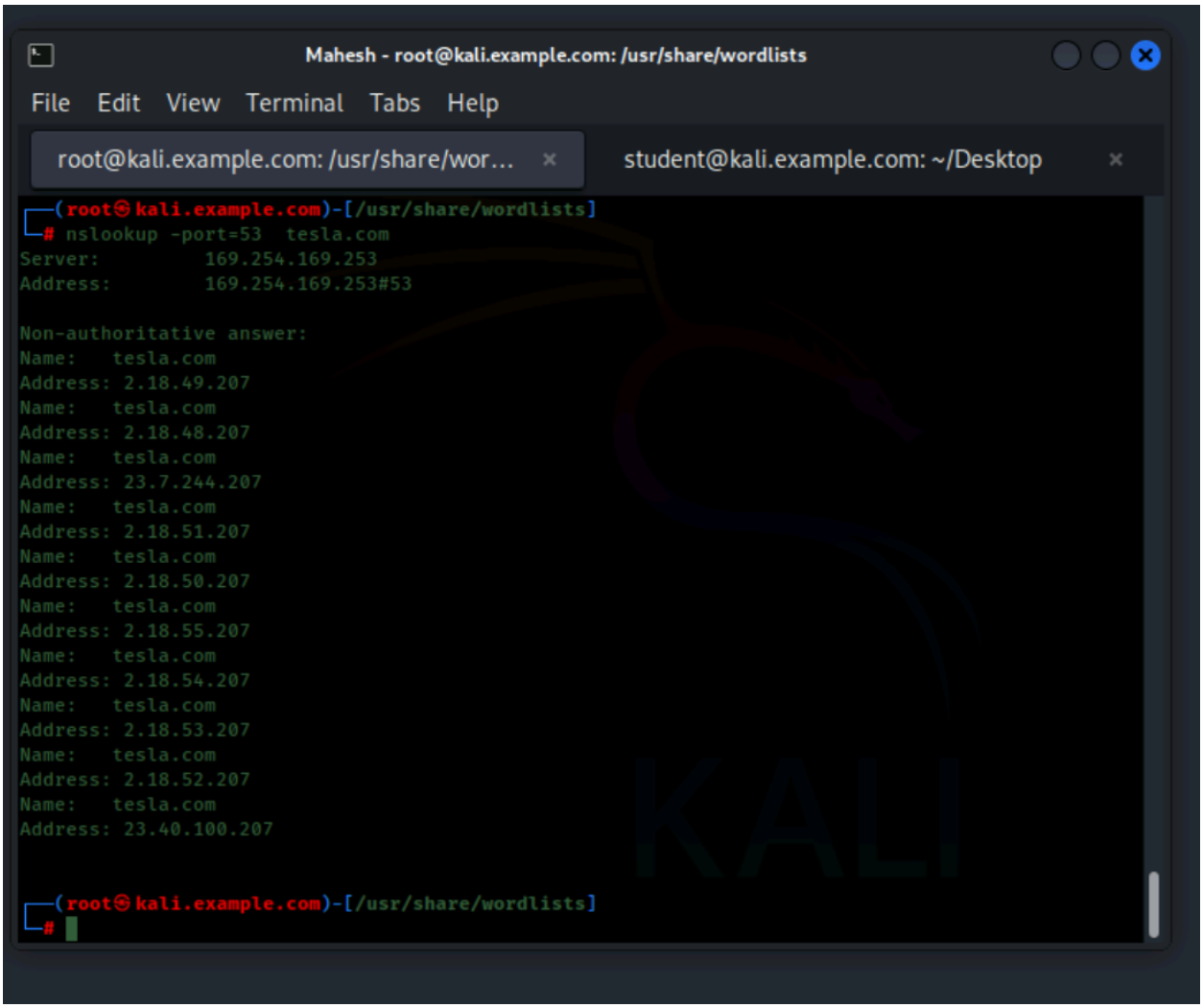
```
nslookup -port=<port number> tesla.com
```

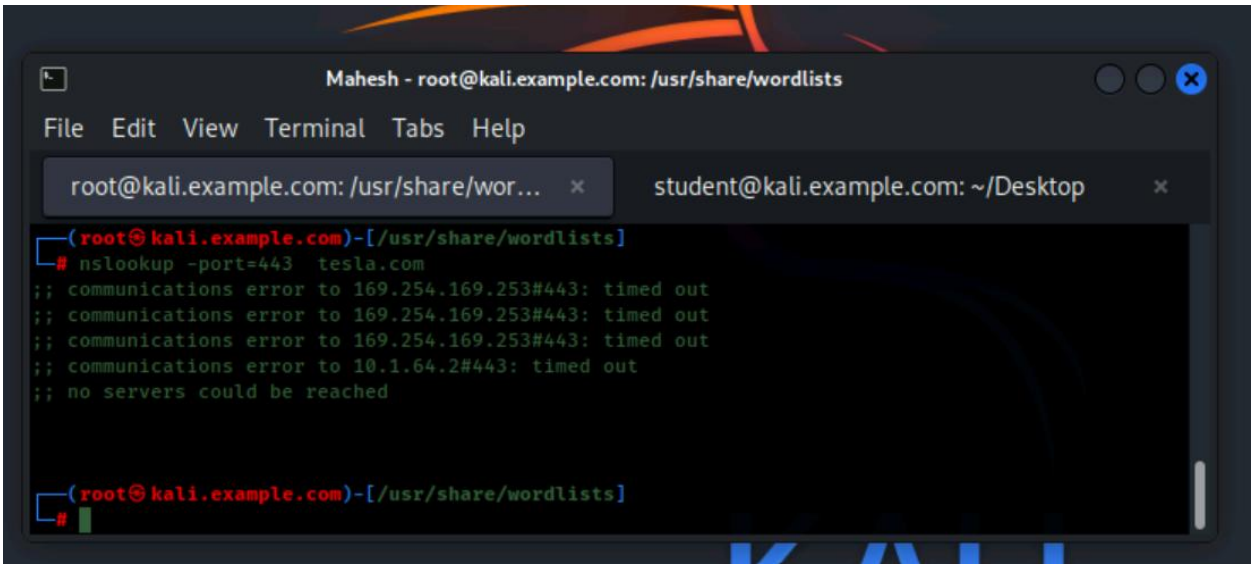
Port 53 is the Nslookup default. Try a few of the common port numbers before moving on. See the image below.

```
┌──(root㉿kali.example.com)-[/usr/share/wordlists
└─# nslookup -port=53 tesla.com
Server:         169.254.169.253
Address:        169.254.169.253#53

Non-authoritative answer:
Name:   tesla.com
Address: 2.18.53.207
Name:   tesla.com
Address: 2.18.54.207
Name:   tesla.com
Address: 2.18.55.207
Name:   tesla.com
Address: 2.18.50.207
Name:   tesla.com
Address: 2.18.51.207
Name:   tesla.com
```

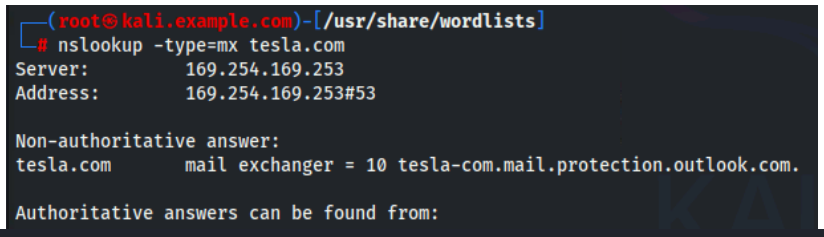
```
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# nslookup -port=443 tesla.com
;; communications error to 169.254.169.253#443: timed out
;; communications error to 169.254.169.253#443: timed out
;; communications error to 169.254.169.253#443: timed out
;; communications error to 10.1.128.2#443: timed out
;; no servers could be reached
```

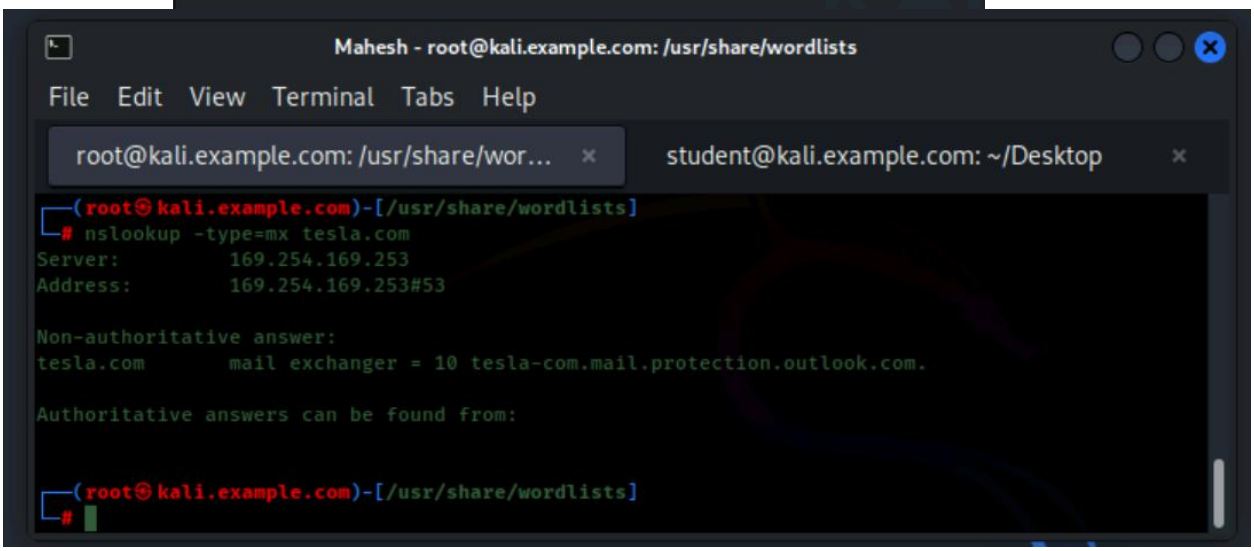




Query for the mail exchanger with the following command:

```
nslookup -type=mx tesla.com
```





This information provides the attacker with the domain to the email server. Tesla is using mimecast. This is an email security management system for Microsoft Exchange. So we now know that Tesla is using Microsoft O365 and Outlook. Crafting exploits will be completed with details of this information. Especially, when it comes to HTML email design.

Task 3: Enum4Linux enumeration

As shown in the PowerPoint Presentation, enum4linux is another easy-to-use enumeration tool. As a penetration tester and ethical hacker you will test systems with many tools and report what was discovered to the organization. Scans that are attempted and do not succeed are not always reported. This depends on the organization's expectations. It is important to have clear expectations before completing a job. A full options list for enum4linux can be found by using the command enum4linux and pressing enter. Many tools in Kali will provide you with help using this tactic; however, you can also type enum4linux -h or visit this link.

Type the following at the command prompt and then hit enter:

```
enum4linux -U <Metasploitable IP>
```

This command will discover the users on the server. See below.

```
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# enum4linux -U 10.1.130.245
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux
/ ) on Thu Jun 27 20:27:25 2024

 ==========================================( Target Information )================
========================

Target ........... 10.1.130.245
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 10.1.130.245 )===
========================


[E] Can't find workgroup/domain



 ===================================( Session Check on 10.1.130.245 )===========
========================


[+] Server 10.1.130.245 allows sessions using username '', password ''


 ================================( Getting domain SID for 10.1.130.245 )========
========================

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 ========================================( Users on 10.1.130.245 )===============
========================

index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: chewbacca        Name:   Desc:

user:[chewbacca] rid:[0x3e8]
enum4linux complete on Thu Jun 27 20:27:35 2024
```

```
Mahesh - root@kali.example.com: /usr/share/wordlists
File  Edit  View  Terminal  Tabs  Help
root@kali.example.com: /usr/share/wor...   student@kali.example.com: ~/Desktop

┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# enum4linux -U 10.1.70.221
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Apr  3
 21:47:09 2025

 =========================================( Target Information )=================================
========

Target ........... 10.1.70.221
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===========================( Enumerating Workgroup/Domain on 10.1.70.221 )====================
=======


[E] Can't find workgroup/domain


 ====================================( Session Check on 10.1.70.221 )============================
========


[+] Server 10.1.70.221 allows sessions using username '', password ''


 ================================( Getting domain SID for 10.1.70.221 )=========================
========

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 =========================================( Users on 10.1.70.221 )===============================
========
```

```
Mahesh - root@kali.example.com: /usr/share/wordlists
File  Edit  View  Terminal  Tabs  Help
root@kali.example.com: /usr/share/wor...   student@kali.example.com: ~/Desktop
========

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 ==========================================( Users on 10.1.70.221 )================================
========

index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: chewbacca        Name:   Desc:

user:[chewbacca] rid:[0x3e8]
enum4linux complete on Thu Apr  3 21:47:20 2025


┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─#
```

Type **`enum4linux -S <Metasploitable IP>`** at the command prompt and then hit enter. This command will discover shares. See below.

```
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# enum4linux -S 10.1.130.245
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux
/ ) on Thu Jun 27 20:32:09 2024

 ==========================================( Target Information )================
=========================

Target ........... 10.1.130.245
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 10.1.130.245 )===
=========================


[E] Can't find workgroup/domain



 ===================================( Session Check on 10.1.130.245 )===========
=========================


[+] Server 10.1.130.245 allows sessions using username '', password ''


 ================================( Getting domain SID for 10.1.130.245 )========
=========================

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 ================================( Share Enumeration on 10.1.130.245 )=========
=========================

do_connect: Connection to 10.1.130.245 failed (Error NT_STATUS_IO_TIMEOUT)

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        public          Disk      WWW
        IPC$            IPC       IPC Service (target server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.1.130.245

//10.1.130.245/print$   Mapping: DENIED Listing: N/A Writing: N/A
//10.1.130.245/public   Mapping: DENIED Listing: N/A Writing: N/A

[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

Mahesh - root@kali.example.com: /usr/share/wordlists

File Edit View Terminal Tabs Help

root@kali.example.com: /usr/share/wor... | student@kali.example.com: ~/Desktop

```
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# enum4linux -S 10.1.70.221
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Apr  3
 21:52:45 2025

 ==========================================( Target Information )================================
========

Target ........... 10.1.70.221
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 10.1.70.221 )=====================
=======


[E] Can't find workgroup/domain



 ====================================( Session Check on 10.1.70.221 )===========================
========


[+] Server 10.1.70.221 allows sessions using username '', password ''


 ================================( Getting domain SID for 10.1.70.221 )========================
========

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 ==================================( Share Enumeration on 10.1.70.221 )=========================
```

```
[+] Can't determine if host is part of domain or part of a workgroup


 ================================( Share Enumeration on 10.1.70.221 )=========================
========

do_connect: Connection to 10.1.70.221 failed (Error NT_STATUS_IO_TIMEOUT)

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        public          Disk      WWW
        IPC$            IPC       IPC Service (target server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.1.70.221

//10.1.70.221/print$    Mapping: DENIED Listing: N/A Writing: N/A
//10.1.70.221/public    Mapping: DENIED Listing: N/A Writing: N/A

[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.1.70.221/IPC$      Mapping: N/A Listing: N/A Writing: N/A
enum4linux complete on Thu Apr  3 21:53:01 2025


┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─#
```

Type **`enum4linux -l <Metasploitable IP>`** at the command prompt and then hit enter. This command will discover information using LDAP port 389. See below.

```
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# enum4linux -l 10.1.130.245
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux
/ ) on Thu Jun 27 20:34:23 2024

 ==========================================( Target Information )================
==========================

Target ........... 10.1.130.245
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 10.1.130.245 )===
==========================


[E] Can't find workgroup/domain


 ===================================( Session Check on 10.1.130.245 )============
========================


[+] Server 10.1.130.245 allows sessions using username '', password ''


 ==========================( Getting information via LDAP for 10.1.130.245 )===
========================


[+] 10.1.130.245 appears to be a child DC


 ================================( Getting domain SID for 10.1.130.245 )========
========================

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup

enum4linux complete on Thu Jun 27 20:34:34 2024
```

```
Mahesh - root@kali.example.com: /usr/share/wordlists
File  Edit  View  Terminal  Tabs  Help
root@kali.example.com: /usr/share/wor...   student@kali.example.com: ~/Desktop

┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# enum4linux -l 10.70.221
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Apr  3
 21:55:21 2025

 =========================================( Target Information )=================================
========

Target ........... 10.70.221
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 10.70.221 )======================
=======


[E] Can't find workgroup/domain


 ====================================( Session Check on 10.70.221 )============================
========


[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.

┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─#
```

Task 4: Using Dig to lookup DNS records

Lookup A records with the following command:

```
dig tesla.com +short
```

```
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# dig tesla.com +short
2.18.54.207
2.18.50.207
2.18.52.207
2.18.48.207
2.18.51.207
23.7.244.207
23.40.100.207
2.18.55.207
2.18.49.207
2.18.53.207
```

```
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# dig tesla.com +short
23.40.100.207
2.18.50.207
2.18.55.207
2.18.48.207
2.18.49.207
2.18.51.207
2.18.53.207
2.18.52.207
2.18.54.207
23.7.244.207
```

Lookup MX records with the following command:

`dig tesla.com MX`

```
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# dig tesla.com MX

; <<>> DiG 9.19.21-1+b1-Debian <<>> tesla.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19451
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;tesla.com.                     IN      MX

;; ANSWER SECTION:
tesla.com.              300     IN      MX      10 tesla-com.mail.protect
ion.outlook.com.

;; Query time: 0 msec
;; SERVER: 169.254.169.253#53(169.254.169.253) (UDP)
;; WHEN: Thu Jun 27 20:42:18 UTC 2024
;; MSG SIZE  rcvd: 88
```

```
Mahesh - root@kali.example.com: /usr/share/wordlists
File  Edit  View  Terminal  Tabs  Help
root@kali.example.com: /usr/share/wor...   student@kali.example.com: ~/Desktop
2.18.52.207
2.18.54.207
23.7.244.207

┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# dig tesla.com MX

; <<>> DiG 9.19.21-1+b1-Debian <<>> tesla.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52077
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;tesla.com.                     IN      MX

;; ANSWER SECTION:
tesla.com.              300     IN      MX      10 tesla-com.mail.protection.outlook.com.

;; Query time: 4 msec
;; SERVER: 169.254.169.253#53(169.254.169.253) (UDP)
;; WHEN: Thu Apr 03 21:56:49 UTC 2025
;; MSG SIZE  rcvd: 88

┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─#
```

Lookup SOA record with the following command:

```
dig tesla.com SOA
```

```
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# dig tesla.com SOA

; <<>> DiG 9.19.21-1+b1-Debian <<>> tesla.com SOA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9142
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;tesla.com.                     IN      SOA

;; ANSWER SECTION:
tesla.com.              39860   IN      SOA     edns69.ultradns.com. noc.teslamotors.com. 2016024
991 1800 86400 86400 86400

;; Query time: 20 msec
;; SERVER: 169.254.169.253#53(169.254.169.253) (UDP)
;; WHEN: Thu Apr 03 21:58:01 UTC 2025
;; MSG SIZE  rcvd: 106
```

Lookup TTL record with the following command:

```
dig tesla.com TTL
```

```
Mahesh - root@kali.example.com: /usr/share/wordlists
File  Edit  View  Terminal  Tabs  Help
root@kali.example.com: /usr/share/wor...   student@kali.example.com: ~/Desktop

┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# dig tesla.com TTL

; <<>> DiG 9.19.21-1+b1-Debian <<>> tesla.com TTL
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22335
;; flags: qr rd ra; QUERY: 1, ANSWER: 10, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;tesla.com.                     IN      A

;; ANSWER SECTION:
tesla.com.              165     IN      A       23.7.244.207
tesla.com.              165     IN      A       2.18.54.207
tesla.com.              165     IN      A       2.18.52.207
tesla.com.              165     IN      A       2.18.53.207
tesla.com.              165     IN      A       2.18.51.207
tesla.com.              165     IN      A       2.18.49.207
tesla.com.              165     IN      A       2.18.48.207
tesla.com.              165     IN      A       2.18.55.207
tesla.com.              165     IN      A       2.18.50.207
tesla.com.              165     IN      A       23.40.100.207

;; Query time: 0 msec
;; SERVER: 169.254.169.253#53(169.254.169.253) (UDP)
;; WHEN: Thu Apr 03 21:58:26 UTC 2025
;; MSG SIZE  rcvd: 198

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 23095
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;TTL.                            IN      A
```

Lookup all DNS Records with the following command:

`dig tesla.com  ANY +noall +answer`

```
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# dig tesla.com  ANY +noall +answer
tesla.com.              221     IN      MX      10 tesla-com.mail.protection.outlook.com.
tesla.com.              221     IN      NS      edns69.ultradns.com.
tesla.com.              221     IN      NS      a10-67.akam.net.
tesla.com.              221     IN      NS      a9-67.akam.net.
tesla.com.              221     IN      NS      a7-66.akam.net.
tesla.com.              221     IN      NS      a1-12.akam.net.
tesla.com.              221     IN      NS      a28-65.akam.net.
tesla.com.              221     IN      NS      a12-64.akam.net.
```

Task 5: Using Dig to complete a DNS zone transfer

This particular task, a zone transfer, **cannot be completed on the Cyber Range**; however, it is important to know and understand how to complete this task in a penetration test.

A zone transfer will provide an attacker with a clear understanding of the internal network.

The site https://digi.ninja/projects/zonetransferme.php is a testing site you can use for this task. First, we will need to know the name of the server. To find this information, we can use the host command. The host command is used to perform DNS lookups. We are using the -t option to specifically perform an nslookup.

- **`host -t ns zonetransfer.me`**

```
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# host -t ns zonetransfer.me
zonetransfer.me name server nsztm2.digi.ninja.
zonetransfer.me name server nsztm1.digi.ninja.
```

```
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# host -t ns zonetransfer.me
zonetransfer.me name server nsztm1.digi.ninja.
zonetransfer.me name server nsztm2.digi.ninja.
```

As you can see there are two servers. To complete a zone transfer, we need to use the -l options. Type the following and press enter:

- **`host -l zonetransfer.me nsztm1.digi.ninja`**

Results from Cyber Range VM:

```
┌──(root㉿kali.example.com)-[/usr/share/nmap/scripts]
└─# host -l zonetransfer.me nsztm1.digi.ninja
;; Connection to 81.4.108.41#53(81.4.108.41) for zonetransfer.me failed: timed o
ut.
;; no servers could be reached

;; Connection to 81.4.108.41#53(81.4.108.41) for zonetransfer.me failed: timed o
ut.
;; no servers could be reached
```

```
┌──(root㉿kali.example.com)-[/usr/share/wordlists]
└─# host -l zonetransfer.me nsztm1.digi.ninja
;; Connection to 81.4.108.41#53(81.4.108.41) for zonetransfer.me failed: timed out.
;; no servers could be reached

;; Connection to 81.4.108.41#53(81.4.108.41) for zonetransfer.me failed: timed out.
;; no servers could be reached
```

Results from a Kali Linux VM OUTSIDE of the Cyber Range:

```
root@kali:~# host -l zonetransfer.me nsztm1.digi.ninja
Using domain server:
Name: nsztm1.digi.ninja
Address: 81.4.108.41#53
Aliases:

zonetransfer.me has address 5.196.105.14
zonetransfer.me name server nsztm1.digi.ninja.
zonetransfer.me name server nsztm2.digi.ninja.
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me domain name pointer www.zonetransfer.me.
asfdbbox.zonetransfer.me has address 127.0.0.1
canberra-office.zonetransfer.me has address 202.14.81.230
dc-office.zonetransfer.me has address 143.228.181.132
deadbeef.zonetransfer.me has IPv6 address dead:beaf::
email.zonetransfer.me has address 74.125.206.26
home.zonetransfer.me has address 127.0.0.1
internal.zonetransfer.me name server intns1.zonetransfer.me.
internal.zonetransfer.me name server intns2.zonetransfer.me.
intns1.zonetransfer.me has address 81.4.108.41
intns2.zonetransfer.me has address 167.88.42.94
office.zonetransfer.me has address 4.23.39.254
ipv6actnow.org.zonetransfer.me has IPv6 address 2001:67c:2e8:11::c100:1332
owa.zonetransfer.me has address 207.46.197.32
alltcpportsopen.firewall.test.zonetransfer.me has address 127.0.0.1
vpn.zonetransfer.me has address 174.36.59.154
www.zonetransfer.me has address 5.196.105.14
```

There you have it, the internal network setup, and the server IP addresses (screenshot below). An attacker can use this information for further scanning, thus increasing the attack surface. This can also help the attacker know what systems to attack from both the outside and the inside if exploited.

Using the Dig tool to complete a zone transfer can reveal data including operating systems, and even notes to the administrators. As shown above, we need to complete a nslookup beforehand to obtain the server name. The syntax for the zone transfer is below.

- **`dig axfr zonetransfer.me @nsztm1.digi.nija`**

```
root@kali:~# dig axfr zonetransfer.me @nsztm1.digi.ninja

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> axfr zonetransfer.me @nsztm1.digi.ninja
;; global options: +cmd
zonetransfer.me.        7200    IN      SOA     nsztm1.digi.ninja. robin.digi.ninja. 2019100801 172800 900 1209600 3600
zonetransfer.me.        300     IN      HINFO   "Casio fx-700G" "Windows XP"
zonetransfer.me.        301     IN      TXT     "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"
zonetransfer.me.        7200    IN      MX      0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      A       5.196.105.14
zonetransfer.me.        7200    IN      NS      nsztm1.digi.ninja.
zonetransfer.me.        7200    IN      NS      nsztm2.digi.ninja.
_sip._tcp.zonetransfer.me. 14000 IN     SRV     0 0 5060 www.zonetransfer.me.
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me. 7200 IN PTR www.zonetransfer.me.
asfdbauthdns.zonetransfer.me. 7900 IN   AFSDB   1 asfdbbox.zonetransfer.me.
asfdbbox.zonetransfer.me. 7200  IN      A       127.0.0.1
asfdbvolume.zonetransfer.me. 7800 IN    AFSDB   1 asfdbbox.zonetransfer.me.
canberra-office.zonetransfer.me. 7200 IN A      202.14.81.230
cmdexec.zonetransfer.me. 300    IN      TXT     "; ls"
contact.zonetransfer.me. 2592000 IN     TXT     "Remember to call or email Pippa on +44 123 4567890 or pippa@zonetransfer.me when
making DNS changes"
dc-office.zonetransfer.me. 7200 IN      A       143.228.181.132
deadbeef.zonetransfer.me. 7201  IN      AAAA    dead:beaf::
dr.zonetransfer.me.     300     IN      LOC     53 20 56.558 N 1 38 33.526 W 0.00m 1m 10000m 10m
DZC.zonetransfer.me.    7200    IN      TXT     "AbCdEfG"
email.zonetransfer.me.  2222    IN      NAPTR   1 1 "P" "E2U+email" "" email.zonetransfer.me.zonetransfer.me.
email.zonetransfer.me.  7200    IN      A       74.125.206.26
Hello.zonetransfer.me.  7200    IN      TXT     "Hi to Josh and all his class"
home.zonetransfer.me.   7200    IN      A       127.0.0.1
Info.zonetransfer.me.   7200    IN      TXT     "ZoneTransfer.me service provided by Robin Wood - robin@digi.ninja. See http://dig
i.ninja/projects/zonetransferme.php for more information."
```