



Cybersecurity

Networking II Challenge Submission File

In a Network Far, Far Away!

Make a copy of this document to work in, and then for each mission, add the solution below the prompt. Save and submit this completed file as your Challenge deliverable.

Mission 1

1. Mail servers for starwars.com:

```
nslookup -querytype=mx starwars.com
```

Linux-Module_default_1678841110859_23677 Clone 1 (Snapshot 1) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal

Mon 16:08

sysadmin@UbuntuDesktop: ~/Des

File Edit View Search Terminal Tabs Help

sysadmin@UbuntuDesktop: ~

sysadmin@UbuntuDesktop: ~

```
sysadmin@UbuntuDesktop:~/Desktop$ man nslookup
```

```
sysadmin@UbuntuDesktop:~/Desktop$ man nslookup
```

```
sysadmin@UbuntuDesktop:~/Desktop$ nslookup -querytype=mx starwars.com
```

```
Server:      8.8.8.8
Address:     8.8.8.8#53
```

```
Non-authoritative answer:
```

```
starwars.com mail exchanger = 5 alt2.aspmx.l.google.com.
starwars.com mail exchanger = 10 aspmx2.googlemail.com.
starwars.com mail exchanger = 1 aspmx.l.google.com.
starwars.com mail exchanger = 10 aspmx3.googlemail.com.
starwars.com mail exchanger = 5 alt1.aspx.l.google.com.
```

```
Authoritative answers can be found from:
```

```
sysadmin@UbuntuDesktop:~/Desktop$
```

2. Explain why the Resistance isn't receiving any emails:

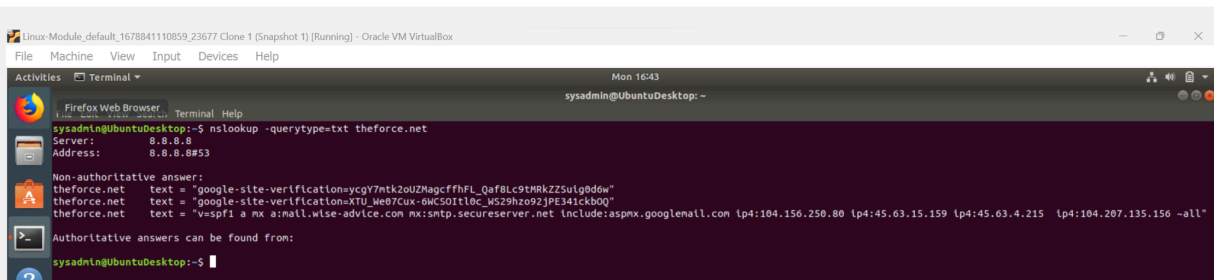
The Resistance is not receiving any emails because the primary and secondary email servers have not been configured correctly.

3. Suggested DNS corrections:

The suggested DNS corrections are to have the proper mail servers set up.
Primary Mail Server= 1 asltx.google.com
Secondary Mail Server= 5 asltx.2.google.com

Mission 2

1. Sender Policy Framework (SPF) of theforce.net:



```
Linux-Module_default_1678841110859_23677 Clone 1 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Firefox Web Browser Terminal Help
sysadmin@UbuntuDesktop:~$ nslookup -querytype=txt theforce.net
Server:
8.8.8.8
Address:
8.8.8.8#53
Non-authoritative answer:
theforce.net text = "google-site-verification=ycgY7ntk2ouZMagcFfhFL_QaFBLc9tMRkZZSulg0d0w"
theforce.net text = "google-site-verification=XTU_Me07Cux-6WCS0itl0c_MS29hzo92jPE34ickb0Q"
theforce.net text = "v=spf1 a mx a:mail.wise-advice.com mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215 ip4:104.207.135.156 ~all"
Authoritative answers can be found from:
sysadmin@UbuntuDesktop:~$
```

```
theforce.net text = "v=spf1 a mx a:mail.wise-advice.com
mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:104.156.250.80
ip4:45.63.15.159 ip4:45.63.4.215 ip4:104.207.135.156 ~all"
```

2. Explain why the Force's emails are going to spam:

The force's emails are going to spam because the IP address changes while the network was down. The new IP is 45.23.176.21 which has not been changed on the SPF record for theforce.net to allow emails.

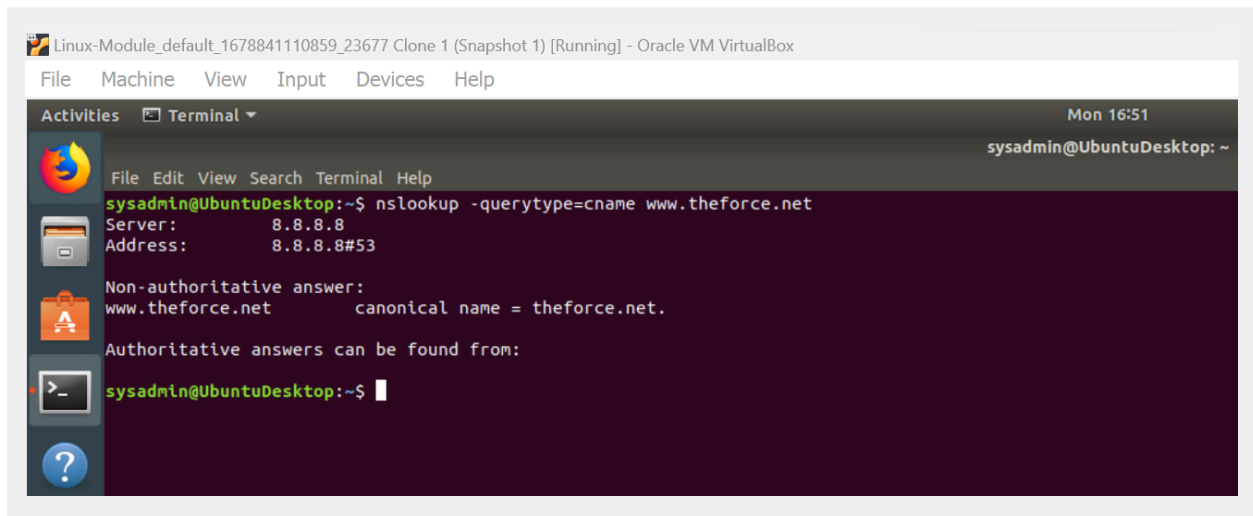
3. Suggested DNS corrections:

The corrections for this DNS record is to add the new IP address to the record which would look like the following:
theforce.net text = "v=spf1 a mx a:mail.wise-advice.com
mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:104.156.250.80

```
ip4:45.63.15.159 ip4:45.63.4.215 ip4:104.207.135.156 ip4: 45.23.176.21  
~all"
```

Mission 3

1. Document the CNAME records:



```
Linux-Module_default_1678841110859_23677 Clone 1 (Snapshot 1) [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
Activities Terminal Mon 16:51 sysadmin@UbuntuDesktop: ~  
File Edit View Search Terminal Help  
sysadmin@UbuntuDesktop:~$ nslookup -querytype=cname www.theforce.net  
Server:      8.8.8.8  
Address:     8.8.8.8#53  
  
Non-authoritative answer:  
www.theforce.net      canonical name = theforce.net.  
  
Authoritative answers can be found from:  
  
sysadmin@UbuntuDesktop:~$
```

2. Explain why the subpage `resistance.theforce.net` isn't redirecting to theforce.net:

The subpage `resistance.theforce.net` is not redirecting to theforce.net because only www.theforce.net was listed to direct in the cname record which mean it would have to be changed to `resistance.theforce.net`.

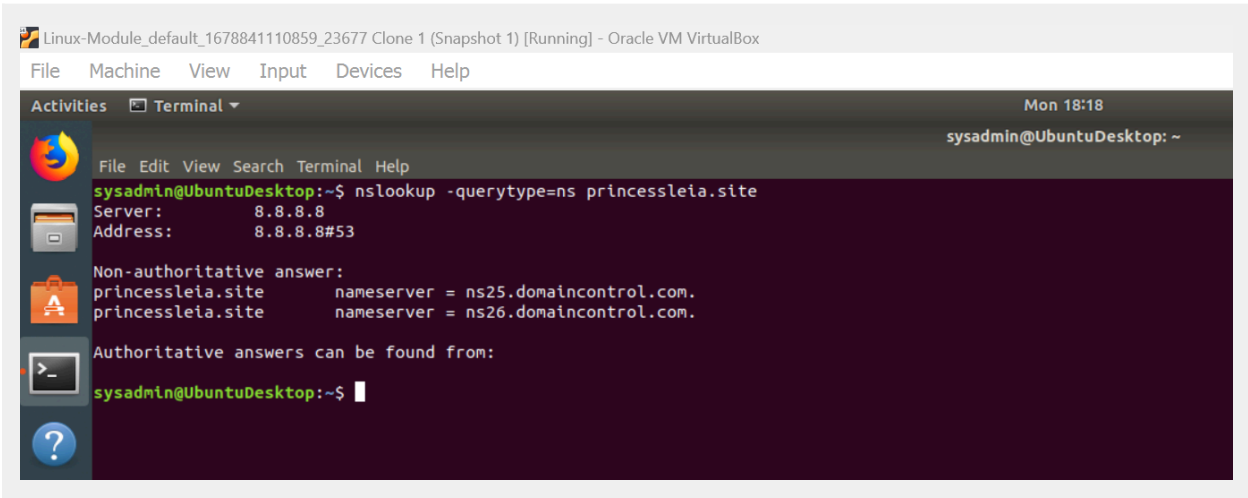
3. Suggested DNS corrections:

The suggested DNS corrections that could be made is to change the cname which would look like the following

www.theforce.net	canonical name - theforce.net
<code>resistance.theforce.net</code>	canonical name - theforce.net

Mission 4

1. Confirm the DNS records for `princessleia.site`:



The screenshot shows a terminal window titled "Linux-Module_default_1678841110859_23677 Clone 1 (Snapshot 1) [Running] - Oracle VM VirtualBox". The terminal is running the command `nslookup -querytype=ns princessleia.site`. The output shows the server as 8.8.8.8 and the address as 8.8.8.8#53. It also displays non-authoritative answers for the nameservers ns25.domaincontrol.com and ns26.domaincontrol.com, and mentions that authoritative answers can be found from:

```
Linux-Module_default_1678841110859_23677 Clone 1 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mon 18:18
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ nslookup -querytype=ns princessleia.site
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
princessleia.site      nameserver = ns25.domaincontrol.com.
princessleia.site      nameserver = ns26.domaincontrol.com.

Authoritative answers can be found from:
sysadmin@UbuntuDesktop:~$
```

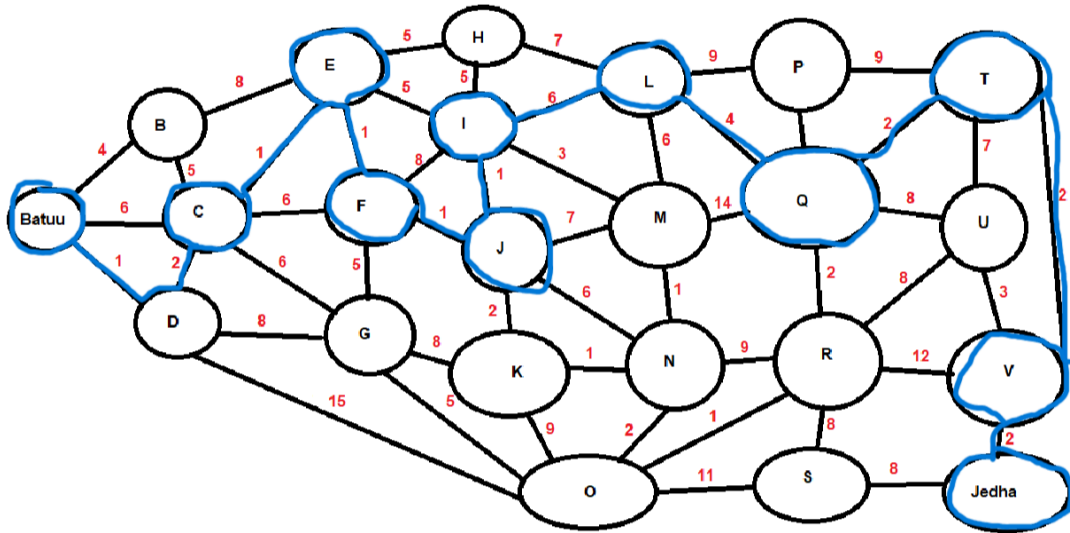
2. Suggested DNS record corrections to prevent the issue from occurring again:

The corrections that would be needed to prevent this from happening again are to create a reference for the backup DNS server.

```
princessleia.site      nameserver=ns2.galaxybackup.com
```

Mission 5

1. Document the shortest OSPF path from Batuu to Jedha:
 - a. OSPF path:



The OSPF path is Batuu-D-C-E-F-J-I-L-Q-T-V-Jedha

b. OSPF path cost:

The cost of the path above is 23

Mission 6

1. Wireless key:

Linux-Module_default_1678841110859_23677 Clone 1 (Snapshot 1) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Mon 18:24 sysadmin@UbuntuDesktop: ~/Desktop

```
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~/Desktop$ aircrack-ng Darkside.pcap -w /usr/share/wordlists/rockyou.txt
Opening Darkside.pcap
Read 586 packets.

# BSSID          ESSID          Encryption
1 00:0B:86:C2:A4:85 linksys        WPA (1 handshake)

Choosing first network as target.
Opening Darkside.pcap
Reading packets, please wait...

Aircrack-ng 1.2 rc4

[00:00:02] 2280/9822769 keys tested (1072.60 k/s)
Time left: 2 hours, 32 minutes, 40 seconds          0.02%

KEY FOUND! [ dictionary ]

Master Key   : 5D F9 20 B5 48 1E D7 05 38 DD 5F D0 24 23 D7 E2
              52 22 05 FE EE BB 97 4C AD 08 A5 2B 56 13 ED E2

Transient Key : 1B 7B 26 96 03 F0 6C 6C D4 03 AA F6 AC E2 81 FC
              55 15 9A AF BB 3B 5A A8 69 05 13 73 5C 1C EC E0
              A2 15 4A E0 99 6F A9 5B 21 1D A1 8E 85 FD 96 49
              5F B4 97 85 67 33 87 B9 DA 97 97 AA C7 82 8F 52

EAPOL HMAC   : 6D 45 F3 53 8E AD 8E CA 55 98 C2 60 EE FE 6F 51
```

2. Host IP addresses and MAC addresses:

a. Sender MAC address:

00:13:ce:55:98:ef

b. Sender IP address:

172.16.0.101

c. Target MAC address:

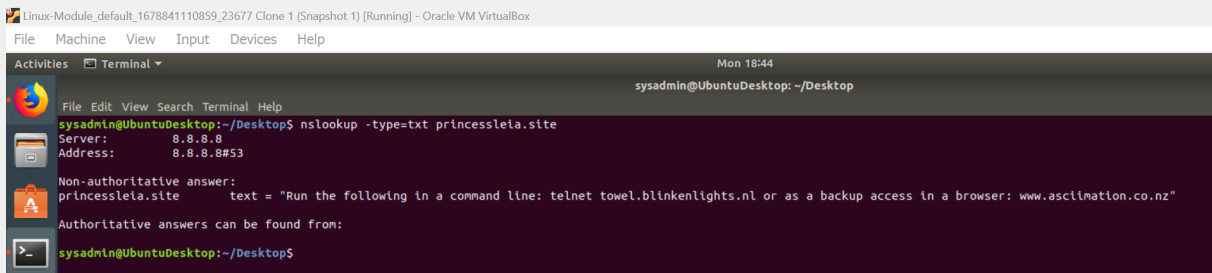
00:13:ce:55:98:ef

d. Target IP address:

172.16.0.1

Mission 7

1. Screenshot of results:



```
Linux-Module_default_1678841110859_23677 Clone 1 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mon 18:44
sysadmin@UbuntuDesktop: ~/Desktop
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~/Desktop$ nslookup -type=txt princessleia.site
Server:      8.8.8.8
Address:     8.8.8.8#53
Non-authoritative answer:
princessleia.site      text = "Run the following in a command line: telnet towel.blinkenlights.nl or as a backup access in a browser: www.asciination.co.nz"
Authoritative answers can be found from:
sysadmin@UbuntuDesktop:~/Desktop$
```

