Cybersecurity

Module 9 Challenge Submission File

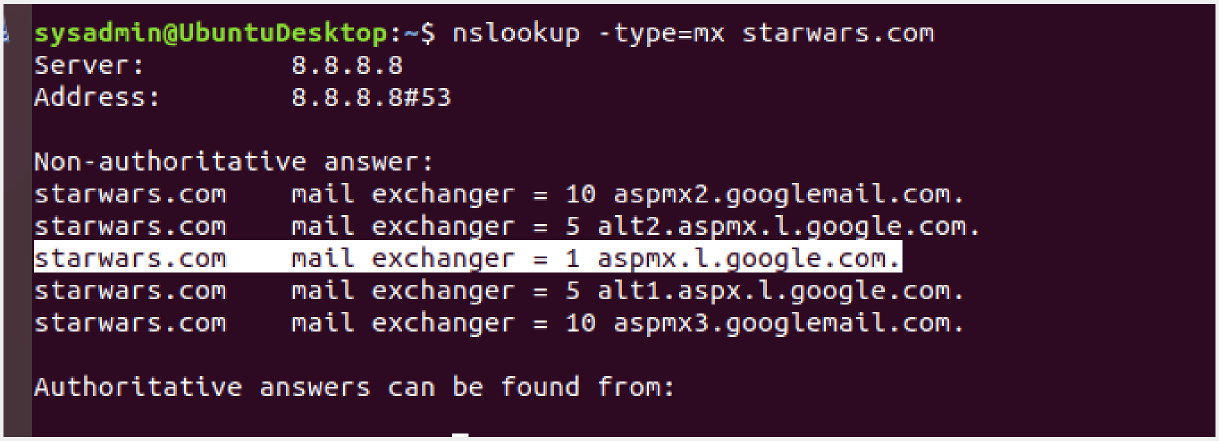
In a Network Far, Far Away!

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:

```
first, I checked the starwars.com domain by entering nslookup -type=mx
starwars.com and here are the results:
```



```
sysadmin@UbuntuDesktop:~$ nslookup -type=mx starwars.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
starwars.com    mail exchanger = 10 aspmx2.googlemail.com.
starwars.com    mail exchanger = 5 alt2.aspmx.l.google.com.
starwars.com    mail exchanger = 1 aspmx.l.google.com.
starwars.com    mail exchanger = 5 alt1.aspx.l.google.com.
starwars.com    mail exchanger = 10 aspmx3.googlemail.com.

Authoritative answers can be found from:
```

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

```
 they are not configured correctly. their primary and secondary servers are not pointing to the asltx.2.google.com and asltx.1.google.com
```

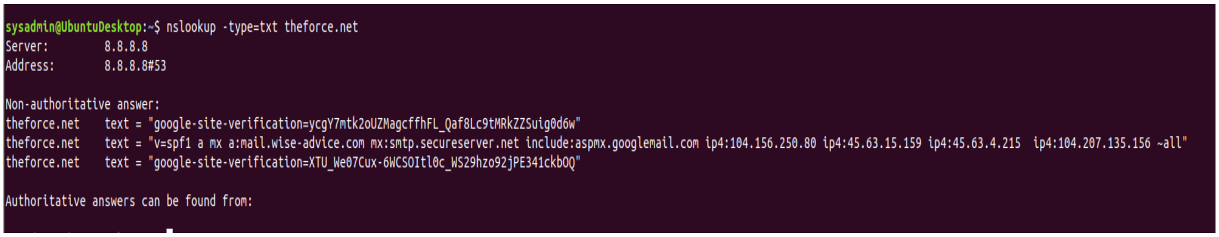
3. Suggested DNS corrections:

```
 starwars.com     mail exchanger = 1 asltx.1.google.com .
 starwars.com     mail exchanger = 5 asltx.2.google.com

```

Mission 2

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

```
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
```



```
sysadmin@UbuntuDesktop:~$ nslookup -type=txt theforce.net
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
theforce.net    text = "google-site-verification=ycgY7mtk2oUZMagcffhFL_Qaf8Lc9tMRkZZSuig0d6w"
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"
theforce.net    text = "google-site-verification=XTU_We07Cux-6WCSOItl0c_WS29hzo92jPE341ckb0Q"

Authoritative answers can be found from:
```

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

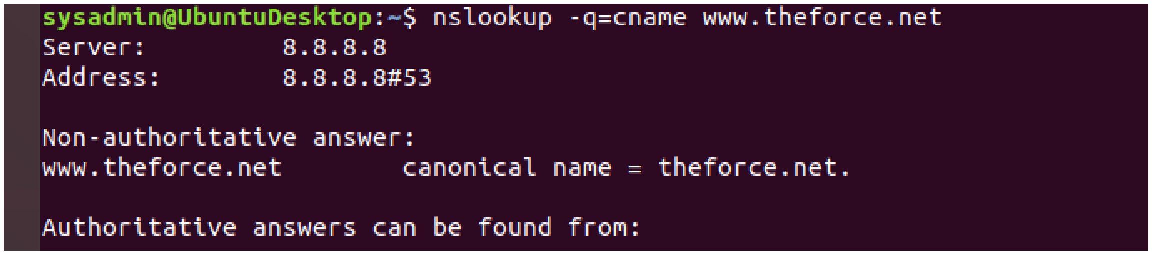
```
IP address 45.23.176.21 is not in the SPF record.
```

3. Suggested DNS corrections:

```
We would have to add IP address 45.23.176.21 to the SPF record.
```

Mission 3

1. Document the CNAME records:



```
sysadmin@UbuntuDesktop:~$ nslookup -q=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:
```

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

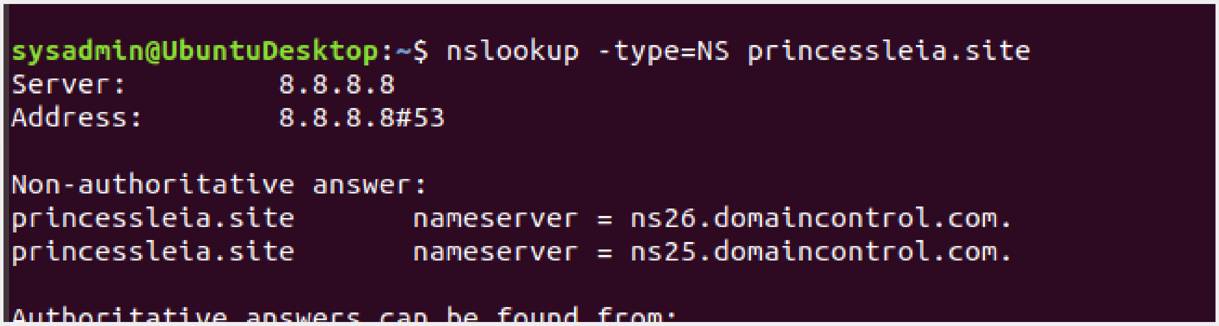
```
resistance.theforce.net isnt pointing to the canonical name
```

3. Suggested DNS corrections:

```
would need to add resistance.theforce.net to theforce.net.
It would look like the following:
resistance.theforce.net       canonical name = theforce.net.
```

Mission 4

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



```
sysadmin@UbuntuDesktop:~$ nslookup -type=NS princessleia.site
Server:         8.8.8.8
Address:        8.8.8.8#53

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

Authoritative answers can be found from:
```

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

```
Add ns2.galaxybackup.com to the nameserver so there would be three.If those
two go down, then the ns2.galaxybackup.com will come up and no change in
service.
```

Mission 5

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

    a. `OSPF` path:

```
Path 1 Battu, D, C, E, F, J, K, N, O, R, Q, T, V, Jedha = 20 (12 hops)
Path 2 Battu, D, C, E, F, J, I, L, Q, T, V, Jedha = 23 (10 hops)
```

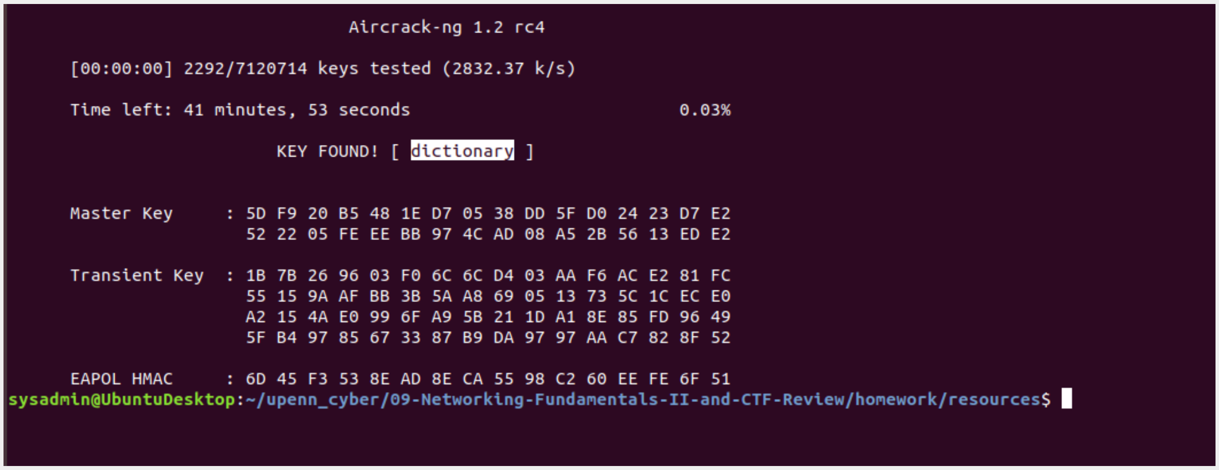
    b. `OSPF` path cost:

```
cheapest is path 1 but the shortest is path 2.
```

Mission 6

1. Wireless key:

ysadmin@UbuntuDesktop:~/upenn_cyber/09-Networking-Fundamentals-II-and-CTF-Review/homework/resources$ aircrack-ng -w /usr/share/wordlists/rockyou.txt Darkside.pcap



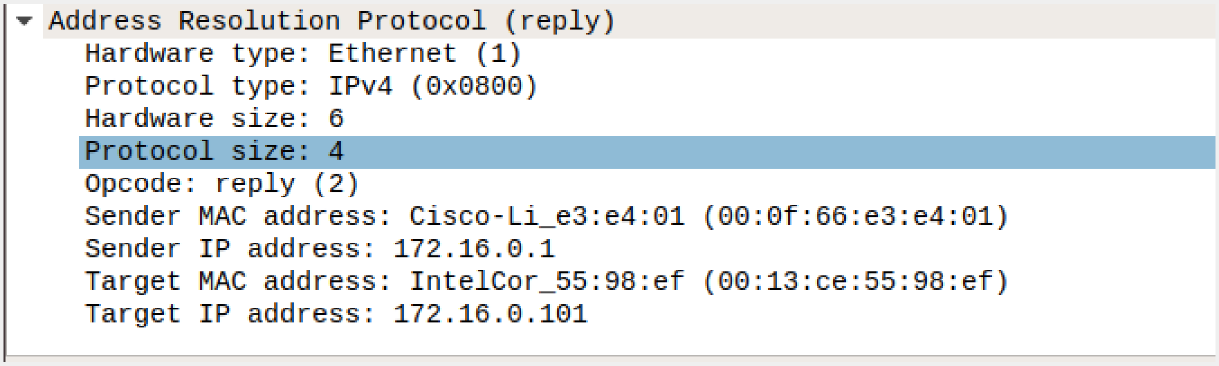
```
                              Aircrack-ng 1.2 rc4

      [00:00:00] 2292/7120714 keys tested (2832.37 k/s)

      Time left: 41 minutes, 53 seconds                          0.03%

                         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
sysadmin@UbuntuDesktop:~/upenn_cyber/09-Networking-Fundamentals-II-and-CTF-Review/homework/resources$
```

2. Host IP addresses and MAC addresses:

    a. Sender MAC address:

Cisco-L1_e3:e4:01 (00:0f:66:e3:e4:01)

```
[Enter text here]
```



```
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Cisco-Li_e3:e4:01 (00:0f:66:e3:e4:01)
    Sender IP address: 172.16.0.1
    Target MAC address: IntelCor_55:98:ef (00:13:ce:55:98:ef)
    Target IP address: 172.16.0.101
```

b. Sender IP address:

```
172.16.0.1
```

c. Target MAC address:

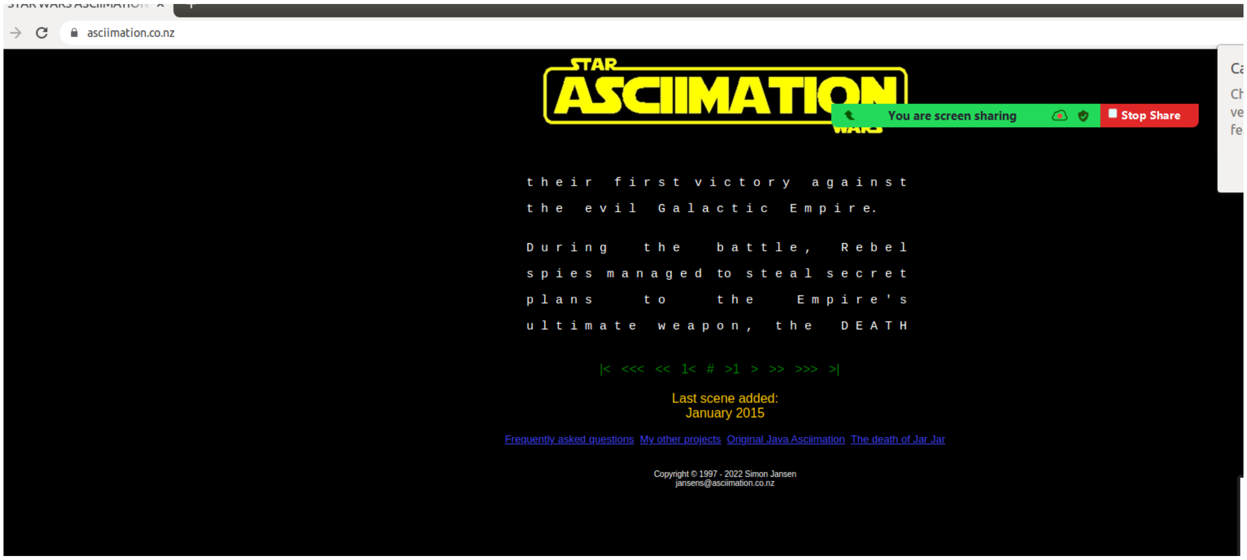
```
IntelCor_55:98:ef (00:13:ce:55:98:ef)
```

d. Target IP address:

```
172.16.0.101
```

Mission 7

1. Screenshot of results:
   ysadmin@UbuntuDesktop:~$ nslookup -type=txt princessleia.site



their first victory against
the evil Galactic Empire.

During the battle, Rebel
spies managed to steal secret
plans to the Empire's
ultimate weapon, the DEATH

|< <<< << 1< # >1 > >> >>> >|

Last scene added:
January 2015

Frequently asked questions My other projects Original Java Asciimation The death of Jar Jar

Copyright © 1997 - 2022 Simon Jansen
jansens@asciimation.co.nz