Cybersecurity

In a Network Far, Far Away!

Mission 1

1. Mail servers for starwars.com:

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

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

```
If the resistance has their mail servers configured to asltx.1.google.com
and asltx.2.google.com, they won't be receiving any because they are going
to the domains listed in question 1.
```

3. Suggested DNS corrections:

They need to change starwars.com mail exchanger =1 asltx.1.google.com and starwars.com mail exchanger=2 asltx.2.google.com

Mission 2

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

Used nslookup -type=txt theforce.net
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:

If the force changed the IP of their mail server to 45.23.176.21 while our network was down, now when we receive emails from them, their IP doesn't have an IP that has an spf record. Not having a SPF record would mean that our mail servers have no way of verifying if these emails are really coming from theforce.net and are classifying them as spam.

3. Suggested DNS corrections:

Theforce.net should add the information from the following to their spf record:

```
sysadmin@UbuntuDesktop:~$ nslookup -type=txt 45.23.176.21
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
21.176.23.45.in-addr.arpa       name = 45-23-176-21.lightspeed.rcsntx.sbcglobal.net.

Authoritative answers can be found from:
```

In summary, their spf record SHOULD read the following the reflect the changes to their mail IP change: Theforce.net text="v=spf1 a mx a:mail.wise-advice.com mx:smtp.secureserver.net include:aspmx.googlemail.com, 45-23-176-21.lightspeed.rcsntx.sbcglobal.net ip4:45.23.176.21 ip4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215 ip4:104.207.135.156

Mission 3

1. Document the CNAME records:

```
sysadmin@UbuntuDesktop:~$ nslookup -type=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.
```

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

```
CNAME acts an alias so that one website can be pointed to another (like
fb.com with facebook.com) however as you can see above there is an absence
of resistance.theforce.net
```

3. Suggested DNS corrections:

```
Resistance.theforce.net should be added to the cname record so that all
traffic sent to resistance will end up at 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.
```

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

```
From the above screenshot, there is no reference to the ns2.galaxybackup.com
when you query princessleia.site. If the resistance wants another layer of
security should princessleia.site go down again, I would recommend adding
the backup server as a name server.
```

Mission 5

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

```
D C E F J I L Q T V then Jedha
```

    b. `OSPF` path cost:

```
Cost is 23
```

Mission 6

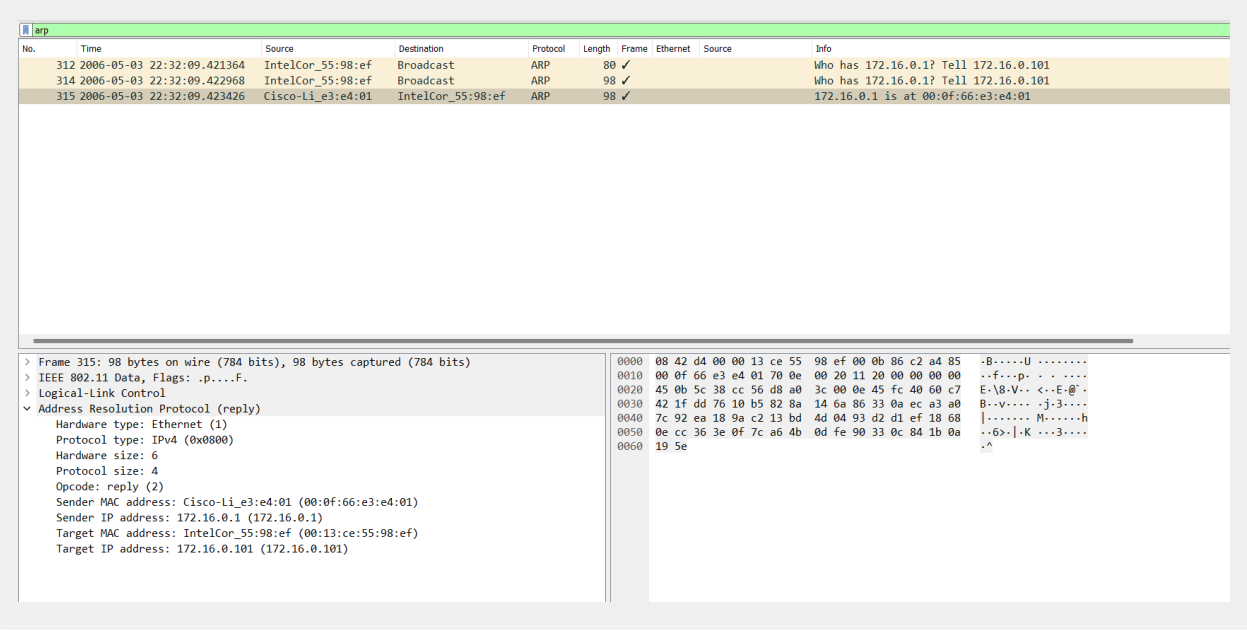
1. Wireless key:

```
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

      [00:00:01] 2280/7120714 keys tested (2002.28 k/s)

      Time left: 59 minutes, 15 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
```

Key is “dictionary”

2. Host IP addresses and MAC addresses:
    a. Sender MAC address:

Cisco-Li_e3:e4:01 (00:0f:66:e3:e4:01) - this was the MAC that responded from our broadcast. Packet 315 as reference



b. Sender IP address:

```
172.16.0.1 - this was the IP that responded from our broadcast
```

c. Target MAC address:

```
IntelCor_55:98:3f (00:13:ce:55:98:ef)
```

d. Target IP address:

```
172.16.0.101
```

Mission 7

1. Screenshot of results:

```
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.asciimation.co
.nz"

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~/Desktop$ telnet towel.blinkenlights.nl
Trying 213.136.8.188...
^C
```

Had to go to the website