

Networks Fundamentals II Homework: In a Network Far, Far Away!

Mission 1

```
nslookup starwars.com
```

```
Server: mynetwork
```

```
Address: 192.168.2.1
```

```
Non-authoritative answer:
```

```
Name: starwars.com
```

```
Addresses: 2001:4958:304::b896:4638
```

```
2001:4958:304::b896:4608
```

```
184.150.70.8
```

```
184.150.70.56
```

So after using NSLOOKUP to check the mail servers this is the result.

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

```
Server: mynetwork
```

```
Address: 192.168.2.1
```

```
Non-authoritative answer:
```

```
starwars.com MX preference = 10, mail exchanger = aspmx3.googlemail.com
```

```
starwars.com MX preference = 5, mail exchanger = alt2.aspmx.l.google.com
```

```
starwars.com MX preference = 5, mail exchanger = alt1.aspx.l.google.com
```

```
starwars.com MX preference = 10, mail exchanger = aspmx2.googlemail.com
```

```
starwars.com MX preference = 1, mail exchanger = aspmx.l.google.com
```

These MX servers were matched to the new primary mail server that the Resistance's network team build which is 'asltx.l.google.com' and the secondary 'asltx.2.google.com', after comparing these to the MX record I conclude that there's configuration issue since the new mail servers don't match with the MX record for starwars.com domain.

The corrected DNS record will have the new primary mail server as 'asltx.l.google.com' and the secondary as 'asltx.2.google.com'.

Mission 2

When we check the SPF records for theforce.net we get the result;

```
nslookup -type=txt
```

Non-authoritative answer:

```
theforce.net text =
```

```
"v=spf1 a mx mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:104.156.250.80  
ip4:45.63.15.159 ip4:45.63.4.215"  
"
```

Which means 104.156.250.80, 45.63.15.159 and 45.63.4.215 are the IP addresses of mail servers allowed to send emails on its behalf.

Now if starwars.com is getting the emails from them with the their new IP 45.23.176.21 it is automatically going to spam since when the receiving email server at starwars.com receives the email, it completes the following steps:

1. Check the sending mail server's IP address, `45.23.176.21`.
2. Validates the DNS record of theforce.net's SPF record to confirm the sending mail server's IP address is either `104.156.250.80 or 45.63.15.159 or 45.63.4.215`.
3. Since the sender's IP is `45.23.176.21` (not `104.156.250.80 or 45.63.15.159 or 45.63.4.215`), starwars.com's mail server can identify the email as spam and potentially reject it or send it to the recipient's spam folder.

The corrected DNS Text Record would contain the IP 45.23.176.21 in the SPF record.

Mission 3

When we look up the cname for www.theforce.com ;

```
nslookup -type=cname www.theforce.net
```

Server: mynetwork

Address: 192.168.2.1

Non-authoritative answer:

```
www.theforce.net canonical name = theforce.net
```

We get the canonical name as theforce.net, and because the domain of the sub page isn't the cname = theforce.net it is not redirecting to www.theforce.net , also by running the nslookup on resistance.theforce.com I determined its not even a valid domain name.

If we correct the DNS record, the cname for theforce.com should be updated to resistance.theforce.com.

Mission 4

The NS record for princessleia.site;

```
nslookup -type=ns princessleia.site
```

```
Server: mynetwork
```

```
Address: 192.168.2.1
```

Non-authoritative answer:

```
princessleia.site    nameserver = ns25.domaincontrol.com
```

```
princessleia.site    nameserver = ns26.domaincontrol.com
```

This confirms which server contains actual DNS records for the domain 'princessleia.site'.

We can update the DNS server and add the backup server 'ns2.galaxybackup.com' to the NS record.

Mission 5

OSPF Shortest path from Batuu to Jedha is Batuu> D > C >E > F > J > M > L > Q > T > V >Jedha which is 29, and this path does not contain Planet N in its route.

Mission 6

I ran

```
aircrack-ng -w /usr/share/wordlists/rockyou.txt Darkside.pcap
```

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] 2280/8053877 keys tested (1574.03 k/s)

Time left: 1 hour, 25 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

Using the key 'dictionary' I decrypted the 802.11 packets captured on the Darkside.pcap file, by editing the Decryption Keys on IEEE 802.11. Then after filtering for ARP packets i determined the Host Mac Address as 00:0f:66:e3:e4:01 and IP address as 172.16.8.1.

The image shows a Wireshark packet capture window titled 'Darkside.pcap'. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons. A filter bar at the top shows 'arp' with a green highlight. Below this is a packet list table with columns: No., Time, Source, Destination, Protocol, Length, Destination Port, and Info.

No.	Time	Source	Destination	Protocol	Length	Destination Port	Info
312	2006-05-03 22:32:09.421364	IntelCor_55:98:ef	Broadcast	ARP	80		Who has 172.16.0.1? Tell 172.16.0.101
314	2006-05-03 22:32:09.422968	IntelCor_55:98:ef	Broadcast	ARP	98		Who has 172.16.0.1? Tell 172.16.0.101
315	2006-05-03 22:32:09.423426	Cisco-Li_e3:e4:01	IntelCor_55:98:ef	ARP	98		172.16.0.1 is at 00:0f:66:e3:e4:01

Below the packet list is a packet details pane for the selected packet (Frame 312). It shows the following structure:

- > Frame 312: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
- > IEEE 802.11 Data, Flags: .p.....T
- ▼ Logical-Link Control
 - > DSAP: SNAP (0xaa)
 - > SSAP: SNAP (0xaa)
 - > Control field: U, func=UI (0x03)
 - Organization Code: 00:00:00 (Officially Xerox, but
 - Type: ARP (0x0006)
- ▼ Address Resolution Protocol (request)
 - Hardware type: Ethernet (1)
 - Protocol type: IPv4 (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - Opcode: request (1)
 - Sender MAC address: IntelCor_55:98:ef (00:13:ce:55:98:ef)
 - Sender IP address: 172.16.0.101 (172.16.0.101)
 - Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
 - Target IP address: 172.16.0.1 (172.16.0.1)

Mission 7

I ran nslookup -type=txt princessleia.site

nslookup -type=txt princessleia.site

Server: 127.0.0.53

Address: 127.0.0.53#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:

Then ran, 'telnet towel.blinkenlights.nl' and got this;

