**Homework 9**

**Mission 1**

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

The old mail servers of starwars.com are:

starwars.com mail exchanger = 10 aspmx3.googlemail.com.

starwars.com mail exchanger = 5 alt1.aspx.l.google.com.

starwars.com mail exchanger = 1 aspmx.l.google.com.

starwars.com mail exchanger = 10 aspmx2.googlemail.com.

starwars.com mail exchanger = 5 alt2.aspmx.l.google.com.

The old mail servers are down and the new mail server is not updated.

**The correct DNS record should have been:**

**starwars.com mail exchanger = asltx.l.google.com**

**starwars.com mail exchanger = asltx.2.google.com**.

**Mission 2**

**nslookup -type=txt theforce.net**

Server: 8.8.8.8

Address: 8.8.8.8#53

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"

theforce.net text = "google-site-verification=ycgY7mtk2oUZMagcffhFL\_Qaf8Lc9tMRkZZSuig0d6w"

theforce.net text = "google-site-verification=XTU\_We07Cux-6WCSOItl0c\_WS29hzo92jPE341ckbOQ"

Authoritative answers can be found from:

The mail is going to spam because **45.23.176.21** is not in the SPF record.

The SPF record of theforce.net should be corrected by including 45.23.176.21.

The correct DNS record should have been:

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 **ipv4:45.23.176.21**"

theforce.net text = "google-site-verification=ycgY7mtk2oUZMagcffhFL\_Qaf8Lc9tMRkZZSuig0d6w"

theforce.net text = "google-site-verification=XTU\_We07Cux-6WCSOItl0c\_WS29hzo92jPE341ckbOQ"

**Mission 3**

nslookup www.theforce.net

Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

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

Name: theforce.net

Address: 104.156.250.80

The cname of www.theforce.net is theforce.net. There is no other cname for the website that resistance.theforce.net cannot be directed to theforce.net.

The correct DNS record should look like:

nslookup www.theforce.net

Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

www.theforce.net canonical name = theforce.net , resistance.theforce.net

Name: theforce.net

Address: 104.156.250.80

**Mission 4**

**nslookup -type=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:

**nslookup -type=soa princessleia.site**

Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

princessleia.site

**origin = ns25.domaincontrol.com**

mail addr = dns.jomax.net

serial = 2021081601

refresh = 28800

retry = 7200

expire = 604800

minimum = 600

* **The primary server of the site is ns25.domaincontrol.com**
* **We need to update the DNS record by adding the backup server:ns2.galaxybackup.com**

**Mission 5**

**Battu-B-E-H-L-Q-U-V-Jeddah**

**Battu-C-F-I-L-Q-U-V-Jeddah**

**MIssion 6**

First I downloaded “**rockyou.txt”dictionary file** and then **aircrack-ng -w rockyou.txt Darkside.pcap**

KEY FOUND! [ **dictionary** ]

**wirehark-open-Darkside.pcacp**

**Wireshark-preference-protocol-IEEE-802-11-edit-add-dictionary:linksys(SSID)**

**Filter ARP**

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**

**Mission 7**

**nslookup -type=txt princessleia.site**

sysadmin@UbuntuDesktop**:~$ telnet towel.blinkenlights.nl**

**Trying 213.136.8.188...**

**Trying 2001:7b8:666:ffff::1:42...**

**telnet: Unable to connect to remote host: Network is unreachable**

