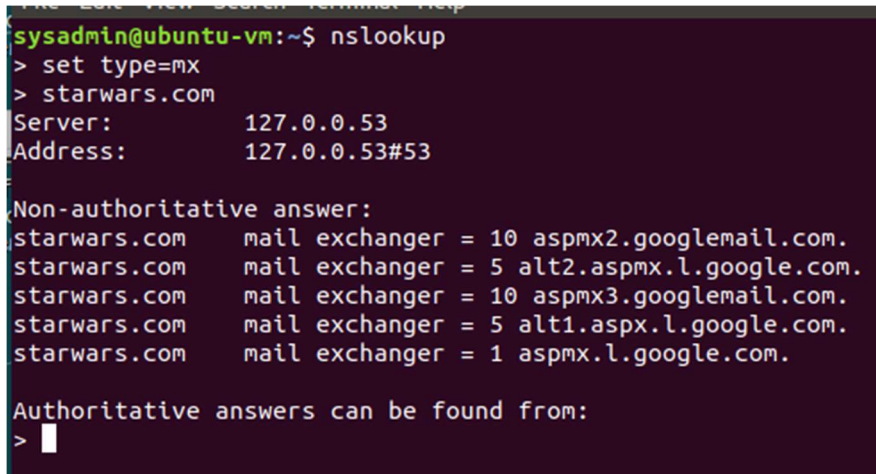


## HOMEWORK #9 – GAVIN FAUGHT

### Mission 1

Using interactive mode of nslookup.

Nslookup → set type=mx → starwars.com

A screenshot of a terminal window with a dark purple background. The prompt is 'sysadmin@ubuntu-vm:~\$'. The user enters 'nslookup', then '> set type=mx', and then '> starwars.com'. The output shows the server and address, followed by a 'Non-authoritative answer:' section listing five mail exchangers for starwars.com with their priorities and names. The prompt '>' is shown at the bottom.

```
sysadmin@ubuntu-vm:~$ nslookup
> set type=mx
> starwars.com
Server:      127.0.0.53
Address:     127.0.0.53#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 = 10 aspmx3.googlemail.com.
starwars.com mail exchanger = 5 alt1.aspx.l.google.com.
starwars.com mail exchanger = 1 aspmx.l.google.com.

Authoritative answers can be found from:
>
```

Mail servers:

- 1 aspmx.l.google.com
- 5 alt1.aspx.l.google.com
- 5 alt2.aspmx.l.google.com
- 10 aspmx2.googlemail.com
- 10 aspmx3.googlemail.com

The resistance isn't receiving any emails because it looks like asltx.1.google.com and asltx.2.google.com are not listed as mail servers. The corrected DNS record should have both asltx.1.google.com and alstx.2.google.com as mail exchangers, ideally:

mail exchanger = 1 asltx.1.google.com  
mail exchanger = 1 asltx.2.google.com

### Mission 2

Using non-interactive mode of nslookup:

Nslookup -type=txt theforce.net

```

sysadmin@ubuntu-vm:~$ nslookup -type=txt theforce.net
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
theforce.net     text = "google-site-verification=XTU_We07Cux-6W
CS0Itl0c_WS29hzo92jPE341ckb0Q"
theforce.net     text = "google-site-verification=ycgY7mtk2oUZMa
gcffhFL_Qaf8Lc9tMRkZZSuig0d6w"
theforce.net     text = "v=spf1 a mx mx:smtp.secureserver.net in
clude:aspmx.googlemail.com ip4:104.156.250.80 ip4:45.63.15.159
ip4:45.63.4.215"

Authoritative answers can be found from:

sysadmin@ubuntu-vm:~$

```

SPF is: text = "v=spf1 a mx mx:smtp.secureserver.net include:aspmx.googlemail.com 1p4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215"

The Force's email is going to spam because the current IP address of their mail server is 45.23.176.21. This IP address is not in the SPF line. A corrected DNS record should look like:

text = "v=spf1 a mx mx:smtp.secureserver.net include:aspmx.googlemail.com 1p4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215 ip4:45.23.176.21"

### Mission 3

Using interactive mode of nslookup:

Nslookup → set type=CNAME → resistance.theforce.net

```

sysadmin@ubuntu-vm:~$ nslookup
> set type=CNAME
> www.theforce.net
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
www.theforce.net canonical name = theforce.net.

Authoritative answers can be found from:
>

```

A CNAME record is a type of DNS record that maps an alias name to a true or canonical domain name.

resistance.theforce.net isn't redirecting to [www.theforce.net](http://www.theforce.net) because there are no aliases when doing a CNAME search. A corrected DNS record should have "resistance.theforce.net" as an alias (CNAME) of www.theforce.net.

## Mission 4

Using: <https://dnschecker.org/all-dns-records-of-domain.php?query=princessleia.site&rtype=ANY>

DNS Records for princessleia.site:

A

princessleia.site

50.63.202.32

599

AAAA

Sorry no record found!

CNAME

Sorry no record found!

MX

Sorry no record found!

NS

Type	Domain Name	NS	TTL
NS	princessleia.site	ns25.domaincontrol.com	3599
NS	princessleia.site	ns26.domaincontrol.com	3599

PTR

Sorry no record found!

SRV

Sorry no record found!

SOA

Type	Domain Name	Primary NS	Responsible Email	TTL
SOA	princessleia.site	ns25.domaincontrol.com	dns.jomax.net	3599

The NS's are ns25.domaincontrol.com and ns26.domaincontrol.com. I would fix the DNS server by adding an NS of "ns2.galaxybackup.com," the backup DNS server provided by the Resistance. This would allow the backup server to operate if ns25 and ns26 are down.

## Mission 5 – Network Traffic

This mission was a lesson learned. When I printed out the map, it didn't print the route from T to V; I have to make sure everything is printed next time I do this. I must have spent an hour analyzing the map without the route from T to V.

Batuu → D → C → E → F → J → I → L → Q → T → V → Jedha (Ideal Route)

$$1 + 2 + 1 + 1 + 1 + 1 + 6 + 4 + 2 + 2 + 2 = \underline{23}$$

## **Mission 6**

Use the command: `aircrack-ng -w rockyou.txt -b 00:0b:86:c2:a4:85 Darkside.pcap`

(Note: rockyou.txt is the wordlist and 00:0b:86:c2:a4:85 is the BSS Id of the first frame)

```

Aircrack-ng 1.2 rc4

[00:00:02] 2280/9822769 keys tested (1118.54 k/s)

Time left: 2 hours, 26 minutes, 23 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
sysadmin@ubuntu-vm:~/Downloads$

```

The Dark Side's key is dictionary. From here, you go to Wireshark. Edit → Preferences → Protocols → IEEE 802.11 → Edit Decryption Keys → Key type = wpa-pwd and Key = dictionary.

MAC Addresses: 00:0f:66:e3:e4:01 and 00:13:ce:55:98:ef

IP Addresses: 172.16.0.1 and 172.16.0.101

## **Mission 7**

Type: `nslookup -type=txt princessleia.site`

```

sysadmin@ubuntu-vm:~/Downloads$ 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"

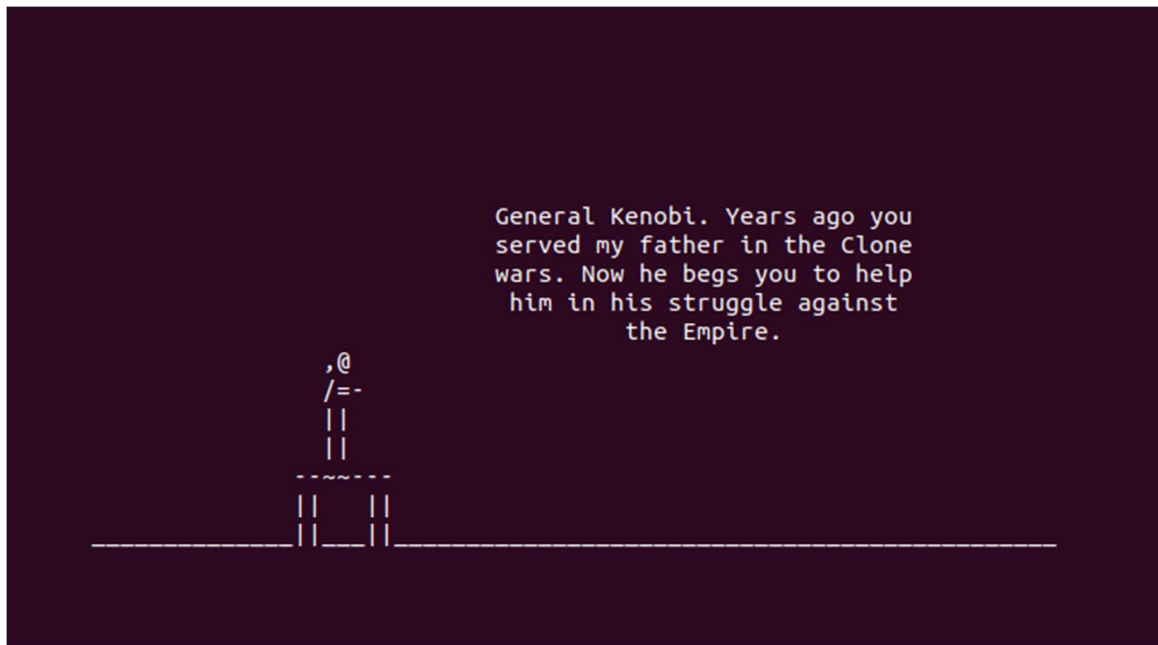
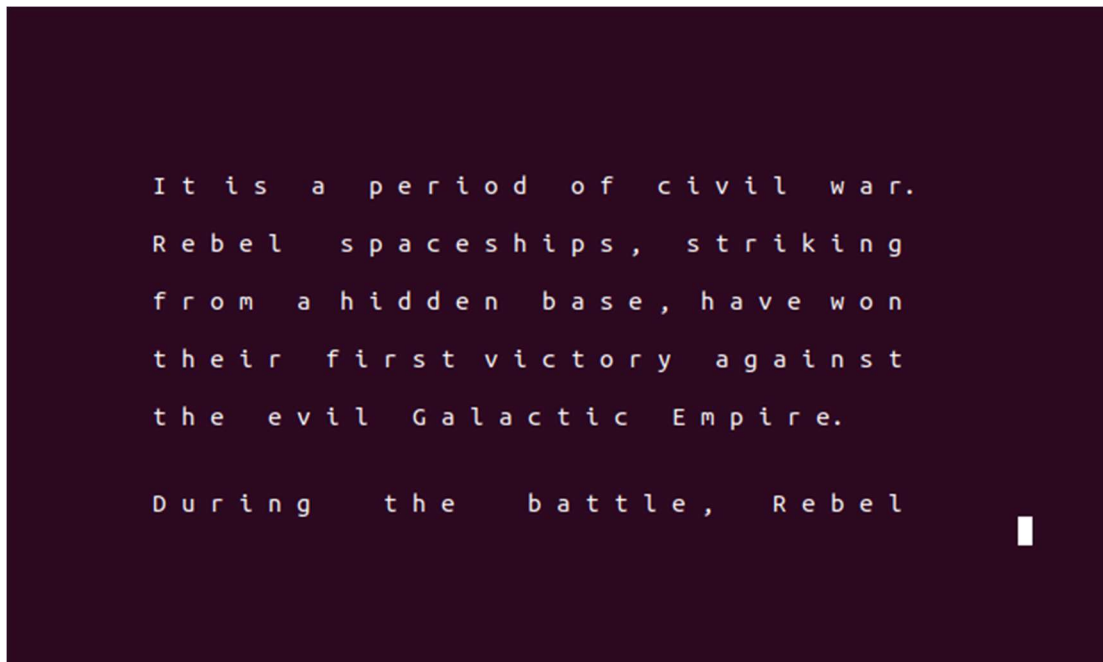
Authoritative answers can be found from:

sysadmin@ubuntu-vm:~/Downloads$

```

Typed: telnet towel.blinkenlights.nl

... it's Star Wars!!! "ASCII"ified!



### Gavin's Corner – Part 1: Use the Force

How to use the Force in real life...well, maybe: <https://www.starwars.com/news/5-force-powers-to-use-in-real-life-situations>

## **Gavin's Corner – Part 2: 10 Most Used nslookup Commands**

- 1) Finding an A record of a domain: `nslookup example.com`
- 2) Checking the NS records of a domain: `nslookup -type=ns example.com`
- 3) Querying a SOA record of a domain: `nslookup -type=soa example.com`
- 4) How to find MX records responsible for email exchange: `nslookup -query=mx example.com`
- 5) Finding all available DNS records of a domain: `nslookup -type=any example.com`
- 6) How to check the using of a specified DNS server: `nslookup example.com ns1.example.com`
- 7) Checking reverse DNS lookup: `nslookup <ip address>`
- 8) Nslookup command to change the port number for the connection:  
`nslookup -port=57 example.com`
- 9) How to change the timeout interval for a reply: `nslookup -timeout=20 example.com`
- 10) How to enable debug mode: `nslookup -debug example.com`

Source: <https://www.cloudns.net/blog/10-most-used-nslookup-commands/>