Cybersecurity

Networking II 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:

```
Non-authoritative answer:
starwars.com      mail exchanger = 10 aspmx2.googlemail.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.
starwars.com      mail exchanger = 5 alt2.aspmx.l.google.com
```

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

```
It appears the DNS records have not been updated with the new mail servers
asltx.1.google.com & asltx.2.google.com
```

3. Suggested DNS corrections:

```
Update DNS MX records to reflect the new mail servers established after the
DoS attack and set the priority as desired for primary/backup.
```

Mission 2

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

```
Server:           8.8.8.8
Address:    8.8.8.8#53

Non-authoritative answer:
theforce.net      text = "v=spf1 a mx a:mail.wise-advice.com
mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:45.63.15.159
ip4:45.63.4.215  ~all"
theforce.net      text =
"google-site-verification=XTU_We07Cux-6WCSOItl0c_WS29hzo92jPE341ckbOQ"
theforce.net      text =
"google-site-verification=ycgY7mtk2oUZMagcffhFL_Qaf8Lc9tMRkZZSuig0d6w"
```

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

```
It appears the new IP address of their mail server, 45.23.176.21, has not
been updated to the DNS records. Therefore, the emails coming from this
unlisted IP are being routed to spam.
```

3. Suggested DNS corrections:

```
Update the DNS SPF records to reflect the new mail server IP so it can be
reconciled and confirmed as a valid sender for theforce.net. At this time,
the listed records should be reviewed to confirm all authorized IP addresses
are listed (if applicable) so this does not happen to other emails that
should be allowed through.
```

Mission 3

1. Document the CNAME records:

```
Server:           8.8.8.8
Address:    8.8.8.8#53
```

```
Non-authoritative answer:
www.theforce.net  canonical name = theforce.net.
theforce.net      nameserver = ns-1.wise-advice.com.
theforce.net      nameserver = ns-2.wise-advice.com.
```

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

```
It appears resistance.theforce.net is not part of the DNS record redirecting
traffic to theforce.net
```

3. Suggested DNS corrections:

```
Update the DNS CNAME records to include resistance.theforce.net and point
this subdomain to the name server theforce.net.
```

Mission 4

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

```
Server:           8.8.8.8
Address:    8.8.8.8#53

Non-authoritative answer:
Name: princessleia.site
Address: 3.33.130.190
Name: princessleia.site
Address: 15.197.148.33
Name: princessleia.site
Address: 20.40.202.19

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.
```

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

```
Create different/additional backup server(s) where the site can be located
as a backup. Then, if the main site goes down, the IP address of the backup
can be temporarily substituted in the main. This would likely be most
effective if the provider/network were different than the primary, such as
mixing in ns#.google.com as opposed to just ns#.domaincontrol.com. If the
main DNS server of one type is taken down, it stands to reason those others
through the same provider may be easily accessed by the hacker as well.
```

Mission 5

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

   a. `OSPF` path:

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

   b. `OSPF` path cost:

```
23
```

Mission 6

1. Wireless key:

```
dictionary
```

2. Host IP addresses and MAC addresses:

   a. Sender MAC address:

```
00:13:ce:55:98:ef
```

b. Sender IP address:

```
172.16.0.101
```

c. Target MAC address:

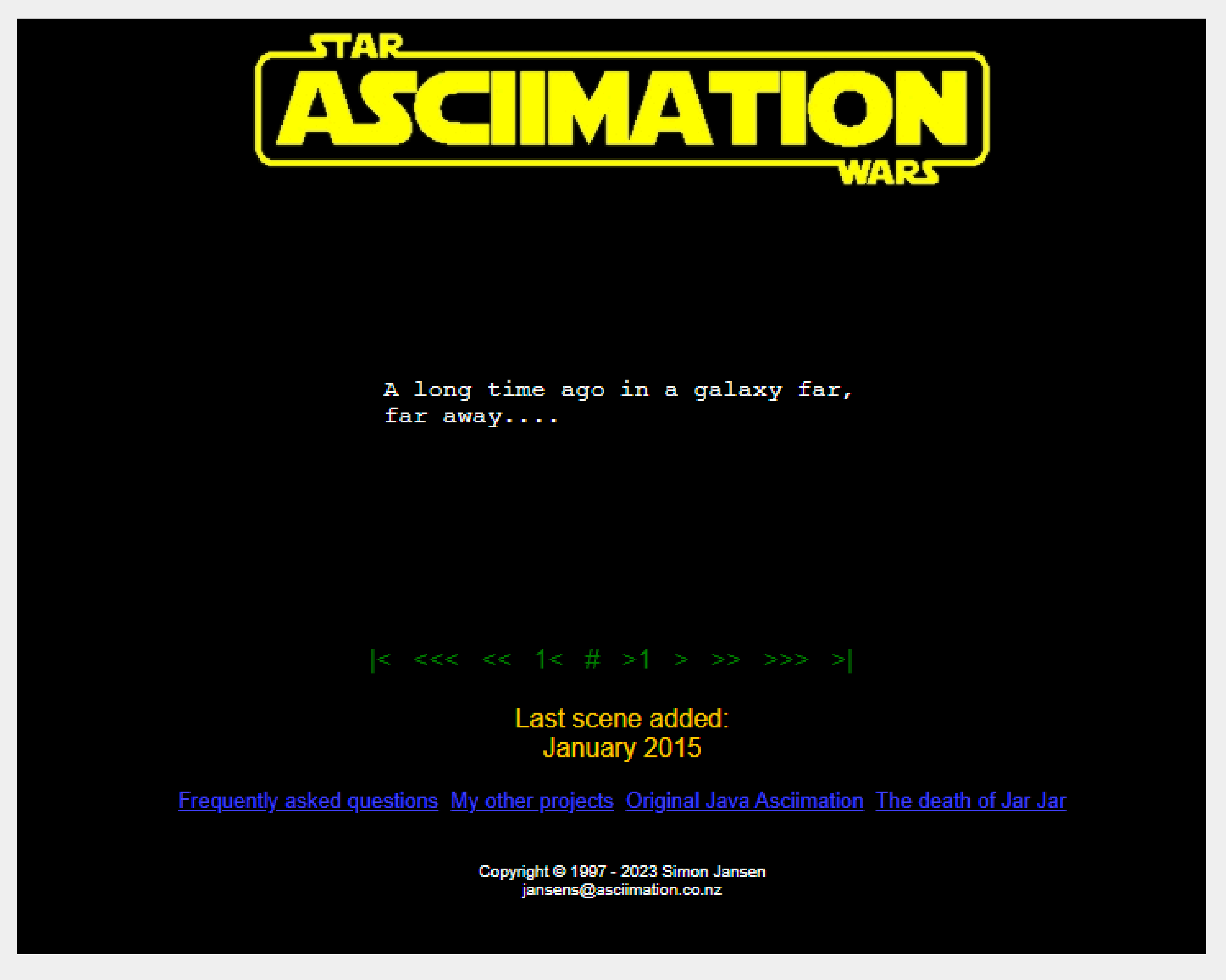
```
00:0f:66:e3:e4:01
```

d. Target IP address:

```
172.16.0.1
```

Mission 7

1. Screenshot of results:



A long time ago in a galaxy far,
far away....

Last scene added:
January 2015

Copyright © 1997 - 2023 Simon Jansen
jansens@asciimation.co.nz