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:

```
nslookup -type=MX starwars.com

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

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

```
The Resistance is unable to receive emails because the primary and secondary
mail servers are still showing alt1.aspx.l.google.com and
alt2.aspmx.l.google.com respectively. These should be updated to
asltx.1.google.com (primary) and asltx.2.google.com (secondary).
```

3. Suggested DNS corrections:

```
To update the Resistance's email servers, they will need to modify the MX
records in the DNS configuration for their domain by changing the primary
server from 'alt1.aspx.l.google.com' to 'asltx.1.google.com' with the
```

```
appropriate priority value and the secondary server from
‘alt2.aspmx.l.google.com’ to ‘asltx.2.google.com’ with a higher priority to
indicate it as a backup. Allow some time for DNS propagation, which
typically takes a few hours to up to 48 hours, for email routing to the
updated servers.
```

Mission 2

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

```
nslookup -type=txt theforce.net

The above command revealed that certain servers and IP addresses, including
‘mail.wise-advice.com’, ‘smtp.secureserver.net’ and specific IP addresses
‘45.63.15.159’ and ‘45.63.4.215’ are authorized to send emails on behalf of
theforce.net. Other sources are neither explicitly allowed nor denied,
denoted by the ‘~all’ qualifier. This SPF record helps prevent email
spoofing and unauthorized use of the domain for sending emails.
```

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

```
After reviewing the SPF using nslookup, it was determined that the Force's
emails are going to spam folders because their SPF record, which specifies
authorized email servers, doesn't include the new IP address (45.23.176.21)
of their mail server. Email providers use SPF records to verify email
legitimacy, and without the updated record, emails are marked as suspicious
and treated as spam.
```

3. Suggested DNS corrections:

```
To fix this issue, theforce.net should update their SPF record to include
the new IP address (45.23.176.21) of their mail server. This will help email
providers recognize their emails as legitimate, reducing the chances of them
ending up in spam folders.
```

Mission 3

1. Document the CNAME records:

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

CNAME - theforce.net

The command above revealed that ‘www.theforce.net’ is a canonical name
(CNAME) for ‘theforce.net’. This means that when you visit
‘www.theforce.net’, it will direct you to the main domain ‘theforce.net’.
```

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

```
The subpage ‘resistance.theforce.net’ is not redirecting to the main domain
‘theforce.net’ because there is no specific CNAME or redirect configured for
it in the DNS settings. Subdomains can have their unique DNS configurations,
and without explicit setup, they won't automatically redirect to the main
domain. To enable this redirection, ‘theforce.net’ needs to establish a
CNAME or another DNS record for ‘resistance.theforce.net’ pointing to
‘theforce.net.’ Additionally, it's worth noting that DNS changes might not
be immediately accessible to all servers due to DNS propagation, which can
take up to 24 hours. During this period, some DNS servers may not yet
recognize the new records (Saturn Cloud, 2023).
```

3. Suggested DNS corrections:

```
To redirect ‘resistance.theforce.net’ to ‘theforce.net’, create a CNAME
record in the DNS provider's control panel with the hostname ‘resistance’
pointing to ‘theforce.net.’ This change tells DNS servers to redirect users
to the main domain when accessing the subpage. DNS changes may take up to 24
hours to fully apply. Also, ensure the CNAME entry is correct, TTL settings
are adjusted if needed, DNS caches are cleared, and use DNS propagation
checkers for verification.
```

Mission 4

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

```
nslookup -type=NS princessleia.site

princessleia.site nameserver = ns25.domaincontrol.com.
princessleia.site nameserver = ns26.domaincontrol.com.
```

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

```
To prevent future DNS outages like the one, it's crucial to add the backup DNS server, ns2.galaxybackup.com, as an additional nameserver (NS) for the domain. This redundancy ensures that if the primary DNS servers (ns25.domaincontrol.com and ns26.domaincontrol.com) fail, the backup server can still resolve DNS queries, guaranteeing continuous access to the site for the Resistance.
```

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:

```
Key: dictionary

ESSID: linksys
```

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

```
Sender MAC address: 00:0f:66:e3:e4:01
```

    b. Sender IP address:

```
Sender IP address: 172.16.0.1
```

    c. Target MAC address:

```
Target MAC address: 00:13:ce:55:98:ef
```

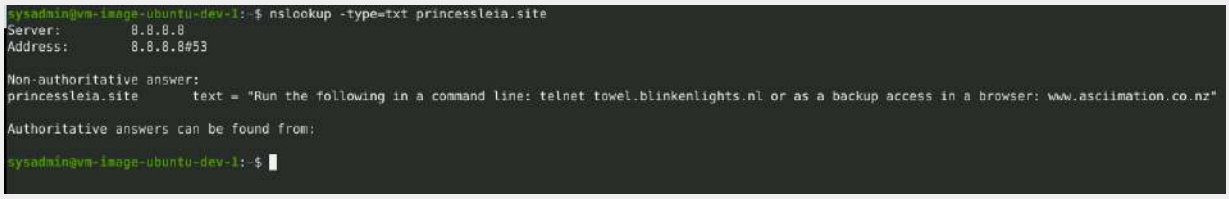
    d. Target IP address:

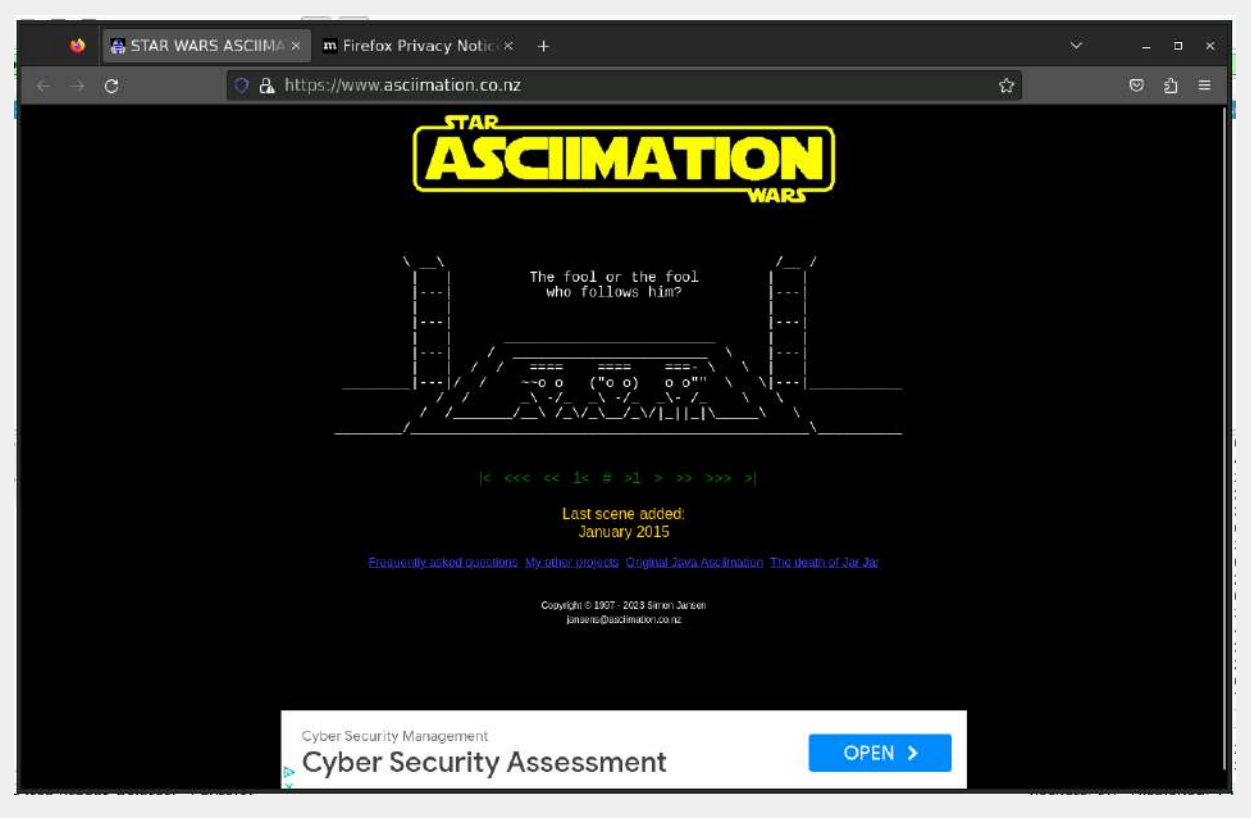
```
Target IP address: 172.16.0.101
```

Mission 7

1. Screenshot of results:

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





References

How to fix CNAME entry not working on namecheap using amazon certificate manager (2023). *Saturn Cloud* https://saturncloud.io/blog/how-to-fix-cname-entry-not-working-on-namecheap-using-amazon-certificate-manager/#:~:text=The%20most%20common%20reason%20for,available%20to%20all%20DNS%20servers.