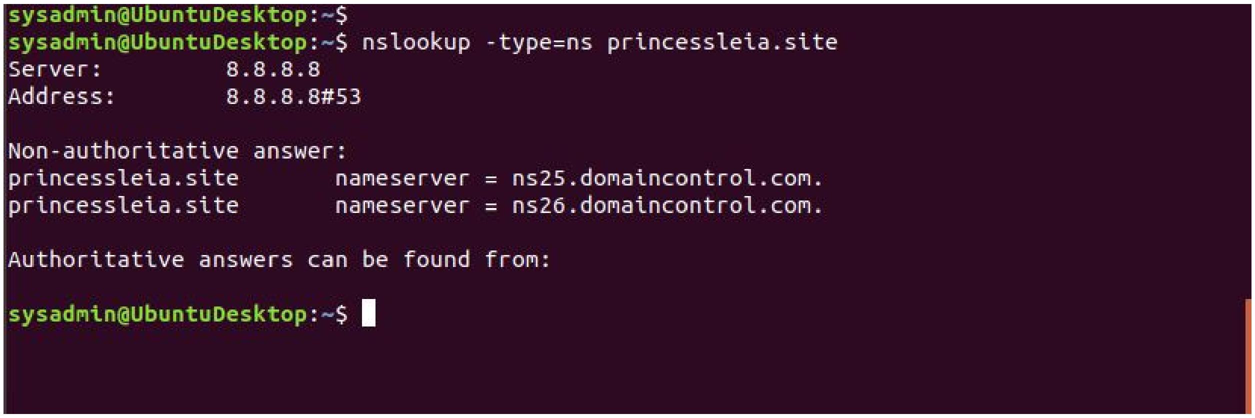
Mission 4

Confirm the DNS records for **princessleia.site.**

Solution:

$ nslookup -type=NS princessleia.site



```
sysadmin@UbuntuDesktop:~$
sysadmin@UbuntuDesktop:~$ 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:

sysadmin@UbuntuDesktop:~$ 
```

Document how you would fix the DNS record to prevent this issue from happening again.

Solution:

The above **nameservers** were taken down during the Empire attack, however there is a backup server **ns2.galaxybackup.com** which must be added as a nameserver to the **princessleia.site** domain.

DNS Management

Log in to **princessleia.site** account
Navigate to **Manage DNS Records** and add the **NS record** of **ns2.galaxybackup.com** provided, to bring up an authoritative nameserver.

Mitigation

1. Restrict **DNS resolver** to only users connected to the local network. This will help to prevent attackers from poisoning the resolver's cache.
2. Keep the **DNS server**, and the **OS** they run patched and updated to prevent them from being exploited due to known vulnerabilities.
3. Ensuring that **DNSSEC** is implemented by the provider. DNSSEC (Domain Name System Security Extensions) by attaching **cryptographic signatures** to the DNS record.
4. Using **two-factor authentication**. If an attacker gains access to one of the administrator’s credentials, access to the DNS will depend on the **second authentication**.
5. **Enable modification locking** that requires specific action before changes can be made.