NCAE competition

SSH

`SSH Server gets public key from SSH client`

- Install ssh for both server and client
  - `sudo apt update`
  - `sudo apt install ssh`
  - `sudo ufw enable`
  - `sudo ufw allow ssh`
- Create an SSH key in the client.
  - `SSH-keygen` —> Make it store in id_rsa.pub
  - Press enter to every prompt
- Copy public key to authorized keys directory (~/.ssh)
  - ssh-copy-id -f bob@192.168.1.26
  - client's public key should be in the authorized key
  - In SSH server, read out the authorized key file.
  - cat ~/.ssh/authorized_keys
  - now ssh

DNS Server

- `cd /etc/bind`
  - If bind does not exist, install bind9
- `sudo nano named.conf.default-zones`
- Add these lines for each domain name and ip address:

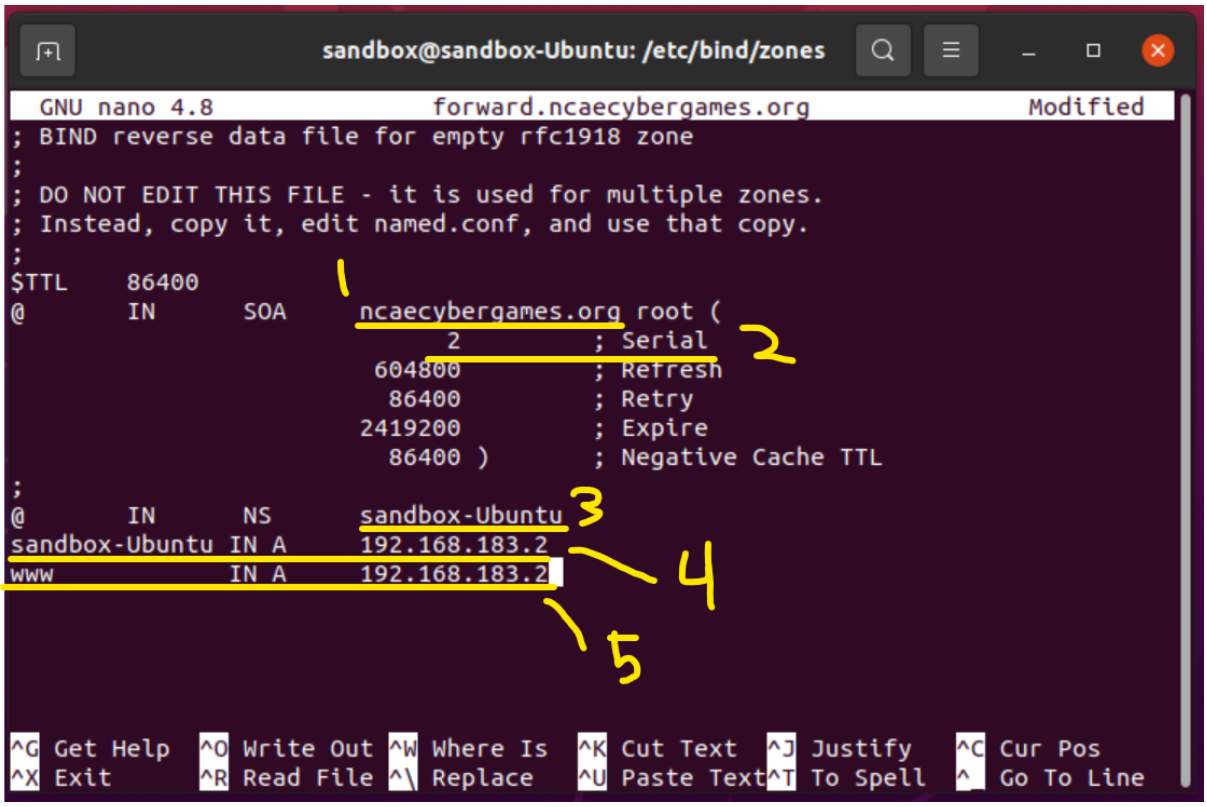
```
zone "<domain_name>" IN {
    type master;
    file "/etc/bind/zones/forward.<domain_name>";
    allow-update { none; };
};

zone "<first parts of ip>.in-addr-arpa" IN {
    type master;
    file "/etc/bind/zones/reverse.<domain_name>";
    allow-update { none; };
};
```

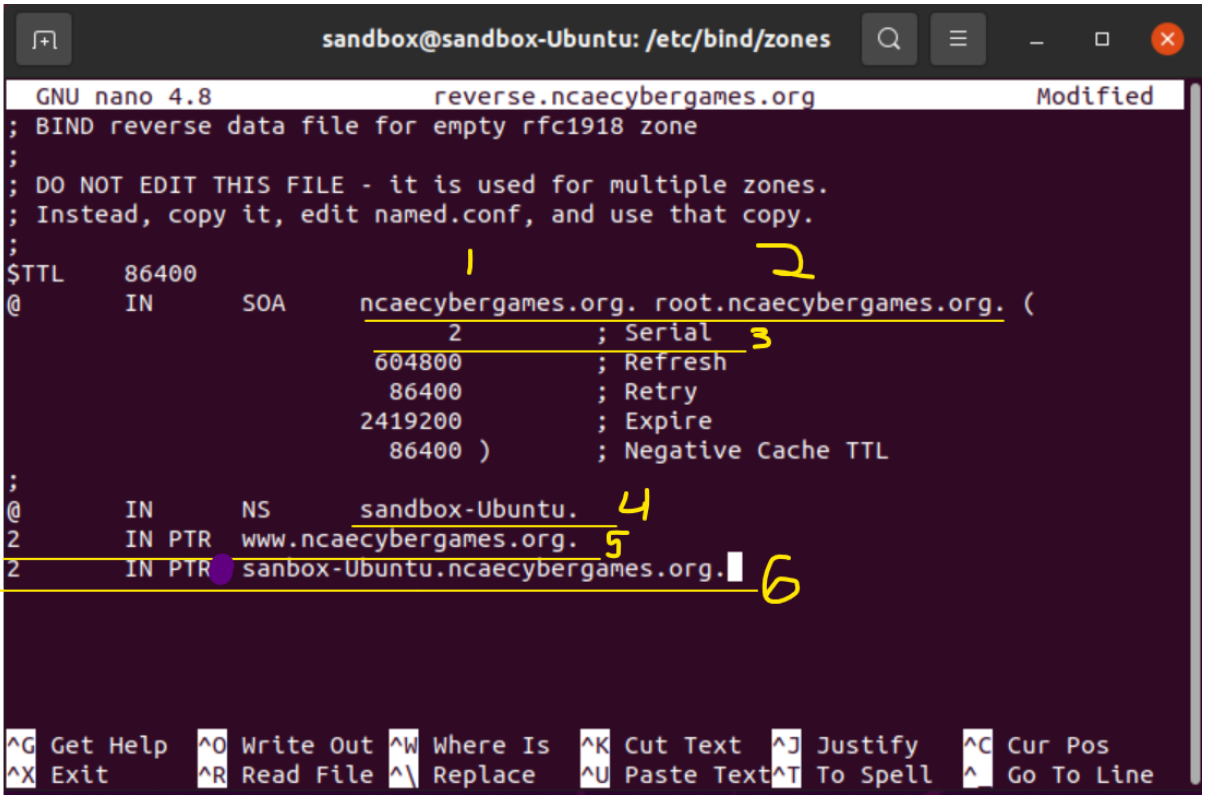
  - Create the forward and reverse files. Copy the db.empy template

```
sudo cp db.empty /etc/bind/zones/forward.<domain_name>
sudo cp db.empty /etc/bind/zones/reverse.<domain_name>
```

- Edit forward.<domain_name>



  - 1: Change from localhost. to <domain_name>
  - 2: Always increment by 1 every time the file is changed
  - 3: Change localhost. to hostname of domain server
  - 4: add the line to resolve the ip of domain server to the domain name
  - 5: add the line to resolve the ip of web server to a www.<domain_name>
- Edit reverse.<domain_name>



- **Note: in reverse lookups, domain names always end with a period.**
- 1: add the domain name
- 2: add domain name with a “root.” in front of it
- 3: increment by 1 every time the file is changed
- 4: add the hostname of domain server
- 5: add this line with last number of the ip of webserver.
- 6: add this line with the last number of the ip of domain server.

- Change dns addresses to the dns server ip through netplan or resolv.conf

```
sudo iptables -F
sudo iptables -F -t nat
sudo iptables -t nat -A PREROUTING -d 172.20.<team_num>.1 -p tcp --dport 80 -j DNAT --to-destination 192.168.<team_num>.2:80
sudo iptables -t nat -A POSTROUTING -j MASQUERADE
```