Lab 10 Template – Ethan Roepke

1. **Screenshot of ssh server active status**
   (5 points)

2. **Three potential services/options to configure. Why or why not configure them.**
   (10 points)

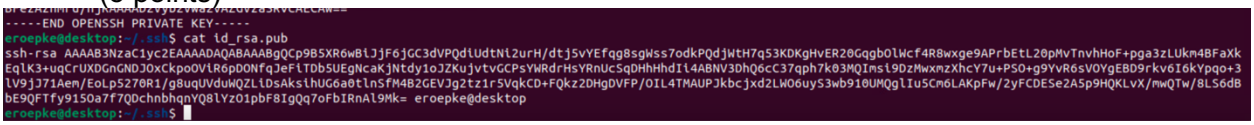
Three potential services to configure SSH server is configuring public key authentication, two-factor authentication, and changing port number. We should configure public key authentication because it is more secure than password based authentication. Users would have to have access to the private key to access the server. This will minimize password based breaches. Configuring a two factor authentication will add an additional layer of protection for users being required to having a time based one time password, as well as the original password. Changing the port number can give a level of security but I think we should not configure them because it can make the administration more complex because you will need to remember the custom port every time you connect.

3. **Screenshot of desktop ssh connection to www2**
   (5 points)

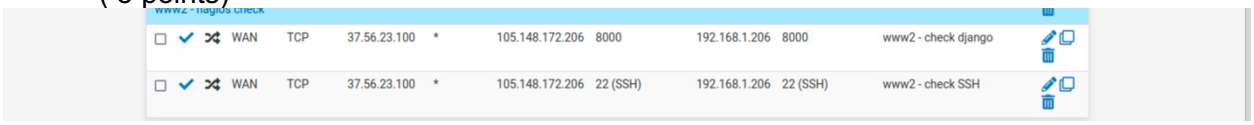
4. **Explain the purpose of the fingerprint and randomart image and when you would use them.**
(10 points)

The randomart image is used to be an easier way for us to validate keys. It is not useful for us, the user but, can be very useful for a user using a connection through SSH to be allowed to connect to the server. Key fingerprint in SSH is a key that is verified when you try to login to a remote computer using SSH.

5. **Screenshot of the public key.**
(5 points)

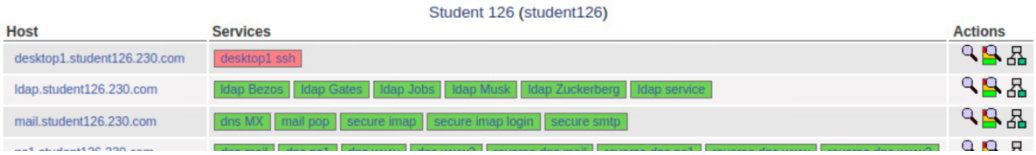


6. **Include a screenshot of your successful NAT rule for ssh on www2.**
(5 points)

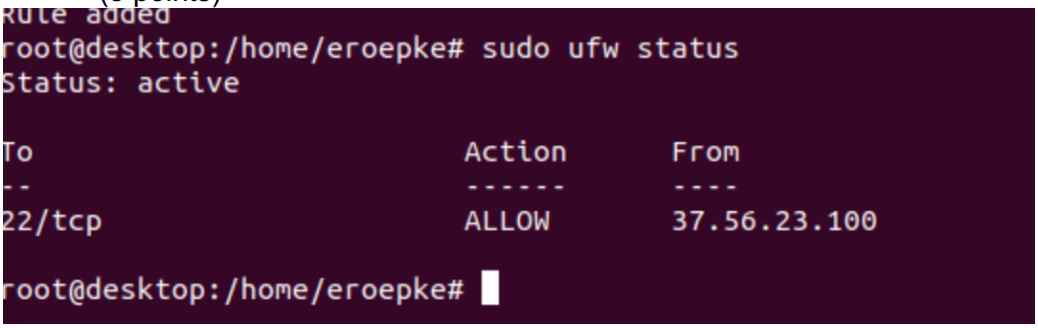


7. **Include a screenshot of the Nagios status showing ssh services are functioning on www2.**
(5 points)

8. **Screenshot of the Nagios services for the desktop with it being red.**
(5 points)



9. **Screenshot of UFW rules for desktop**
(5 points)



10. **Screenshot of the Nagios services for the desktop turning green after UFW rules.**
(5 points)

Student 126 (student126)

Host	Services
desktop1.student126.230.com	desktop1 ssh
ldap.student126.230.com	ldap Bezos, ldap Gates, ldap Jobs, ldap Musk, ldap Zuckerberg

11. **Screenshot of UFW rules for ns2**
(5 points)

```
root@ns2:/home/eroepke# sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
53/udp                     ALLOW       192.168.1.0/24
53/udp                     ALLOW       37.56.23.100

root@ns2:/home/eroepke# _
```

12. **Screenshot of 6 additional sets of UFW rules (ns1, www, mail, ldap, www2, ws)**
(10 points)

Ns1

```
root@ns1:/home/eroepke# sudo ufw allow to any port 53 proto udp
Rule added
root@ns1:/home/eroepke# ufw status
Status: active

To                         Action      From
--                         ------      ----
53/udp                     ALLOW       192.168.1.0/24
53/udp                     ALLOW       37.56.23.100
53/udp                     ALLOW       Anywhere
```

www

```
root@www:/home/cpre230# ufw status
Status: active

To                         Action      From
--                         ------      ----
80/tcp                     ALLOW       192.168.1.0/24
80/tcp                     ALLOW       37.56.23.100
443/tcp                    ALLOW       192.168.1.0/24
443/tcp                    ALLOW       37.56.23.100

root@www:/home/cpre230#
```

mail

```
Rule added
root@mail:/home/cpre230# sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
25/tcp                     ALLOW       192.168.1.0/24
25/tcp                     ALLOW       37.56.23.100
993/tcp                    ALLOW       192.168.1.0/24
993/tcp                    ALLOW       37.56.23.100
110/tcp                    ALLOW       192.168.1.0/24
110/tcp                    ALLOW       37.56.23.100
587/tcp                    ALLOW       192.168.1.0/24
587/tcp                    ALLOW       37.56.23.100

root@mail:/home/cpre230# _
```

ldap

```
Proceed with operation (y|n)? y
Rule deleted
root@ldap:/home/cpre230# ufw status
Status: active

To                         Action      From
--                         ------      ----
389/tcp                    ALLOW       192.168.1.0/24
389/tcp                    ALLOW       37.56.23.100
636/tcp                    ALLOW       37.56.23.100
636/tcp                    ALLOW       192.168.1.0/24

root@ldap:/home/cpre230# _
```

www2

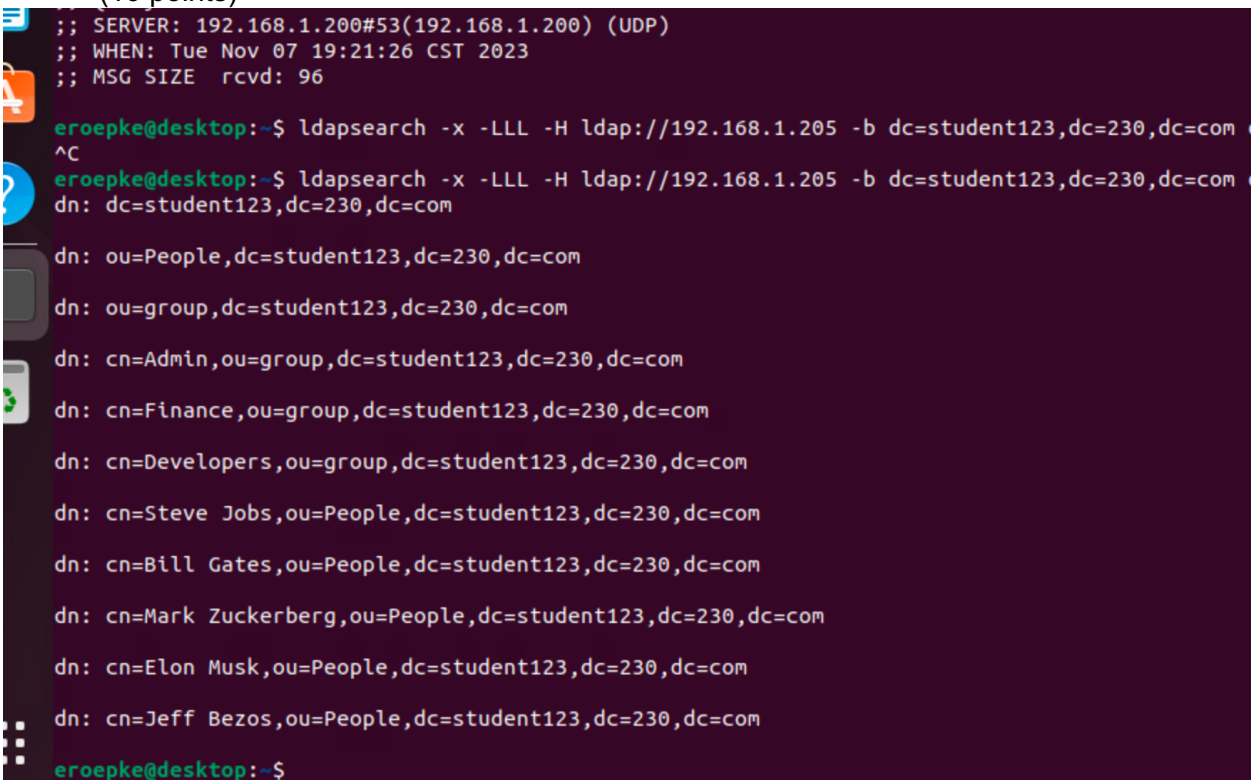
```
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       192.168.1.0/24
22/tcp                     ALLOW       37.56.23.100
22/tcp                     ALLOW       Anywhere
8000/tcp                   ALLOW       Anywhere
```

ws

```
root@workstation:/home/cpre230# ufw status
Status: active
root@workstation:/home/cpre230# ufw status
Status: active
root@workstation:/home/cpre230#
```

13. **Screenshot of successful LDAP query on partner's network.**
(10 points)



14. **Final network diagram.**
(15 points)

Ethan Roepke network diagram