

Lab 10 Template – Ethan Roepke

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

```
No VM guests are running. Detected hypervisor (qemu) binaries on this host.
cpre230@www2:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2023-10-26 17:02:13 UTC; 6 days ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 979 (sshd)
     Tasks: 1 (limit: 1013)
    Memory: 2.6M
       CPU: 25ms
   CGroup: /system.slice/ssh.service
           └─979 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 26 17:02:13 www2 systemd[1]: Starting OpenBSD Secure Shell server...
Oct 26 17:02:13 www2 sshd[979]: Server listening on 0.0.0.0 port 22.
Oct 26 17:02:13 www2 systemd[1]: Started OpenBSD Secure Shell server.
cpre230@www2:~$ 6=
```

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)

```
eroepke@desktop: ~$ ssh cpre230@www2.student126.230.com
The authenticity of host 'www2.student126.230.com (192.168.1.206)' can't be established.
ED25519 key fingerprint is SHA256:9kBFacu/k12yah3FuXglDCzs01jMU4HN4mpDg+klcaI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint]): yes
Warning: Permanently added 'www2.student126.230.com' (ED25519) to the list of known hosts.
cpre230@www2.student126.230.com's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-87-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Thu Nov  2 03:45:03 PM UTC 2023

System load:  0.015625      Processes:            203
Usage of /:   56.7% of 9.75GB Users logged in:      1
Memory usage: 27%          IPv4 address for ens160: 192.168.1.206
Swap usage:   0%

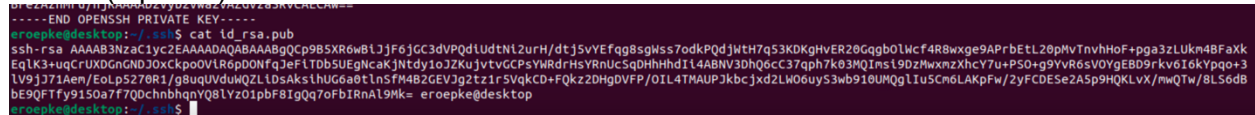
Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.
```

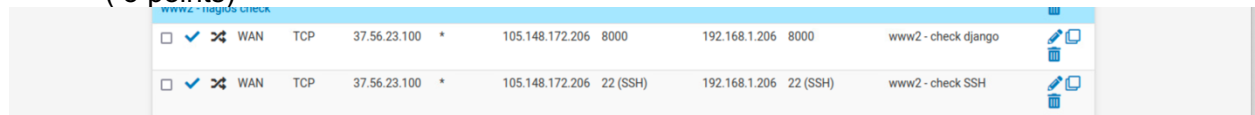
4. Explain the purpose of the fingerprint and randomart image and when you would use them.

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.

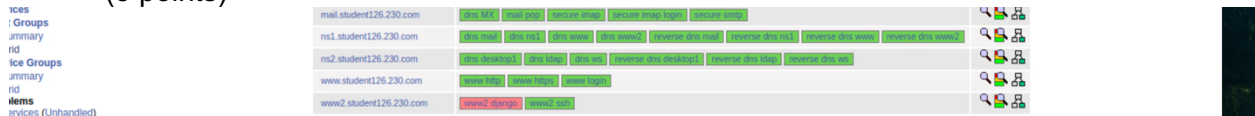
5. **Screenshot of the public key.**
(5 points)



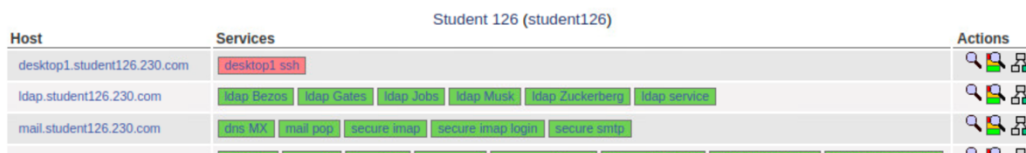
6. **Include a screenshot of your successful NAT rule for ssh on www2.**
(5 points)



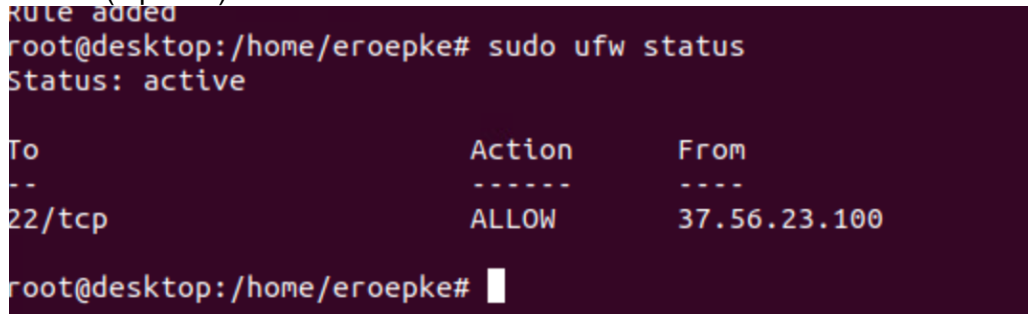
7. Include a screenshot of the Nagios status showing ssh services are functioning on **www2**.
(5 points)



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)

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

```
(be sure to update your notes accordingly)
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)

```
;; SERVER: 192.168.1.200#53(192.168.1.200) (UDP)
;; WHEN: Tue Nov 07 19:21:26 CST 2023
;; MSG SIZE rcvd: 96

eroepke@desktop:~$ ldapsearch -x -LLL -H ldap://192.168.1.205 -b dc=student123,dc=230,dc=com
^C
eroepke@desktop:~$ ldapsearch -x -LLL -H ldap://192.168.1.205 -b dc=student123,dc=230,dc=com
dn: dc=student123,dc=230,dc=com

dn: ou=People,dc=student123,dc=230,dc=com
dn: ou=group,dc=student123,dc=230,dc=com
dn: cn=Admin,ou=group,dc=student123,dc=230,dc=com
dn: cn=Finance,ou=group,dc=student123,dc=230,dc=com
dn: cn=Developers,ou=group,dc=student123,dc=230,dc=com
dn: cn=Steve Jobs,ou=People,dc=student123,dc=230,dc=com
dn: cn=Bill Gates,ou=People,dc=student123,dc=230,dc=com
dn: cn=Mark Zuckerberg,ou=People,dc=student123,dc=230,dc=com
dn: cn=Elon Musk,ou=People,dc=student123,dc=230,dc=com
dn: cn=Jeff Bezos,ou=People,dc=student123,dc=230,dc=com
eroepke@desktop:~$
```

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

Ethan Roepke network diagram

