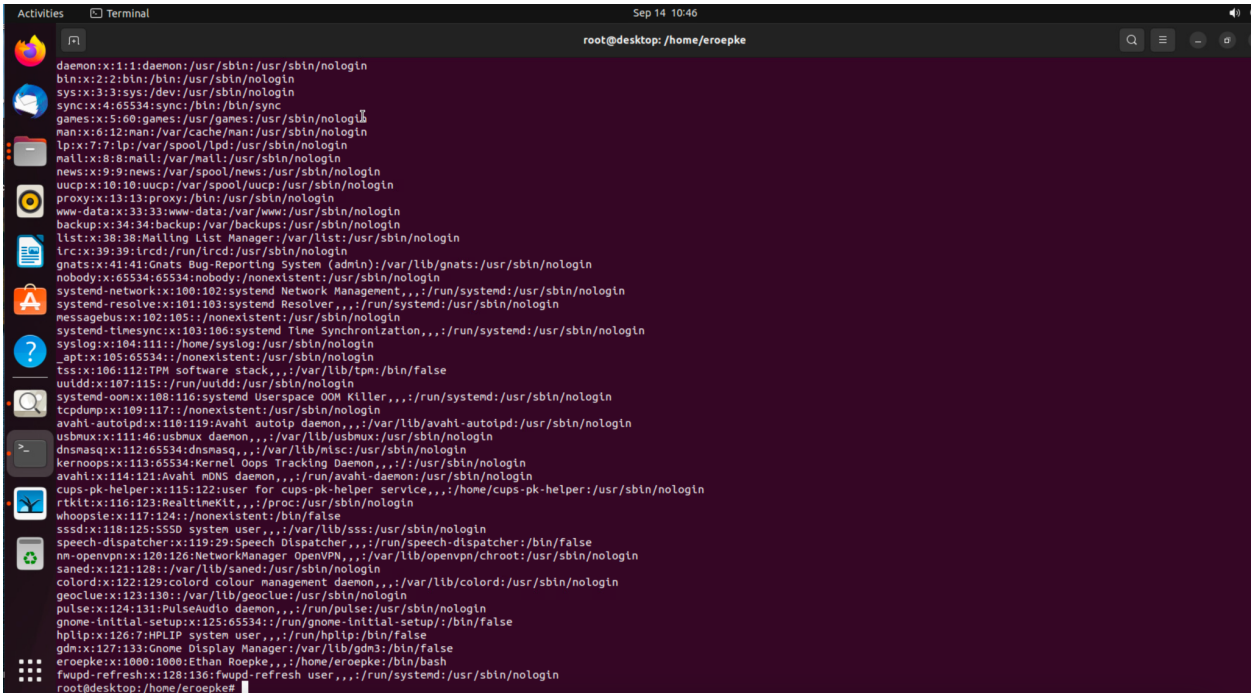
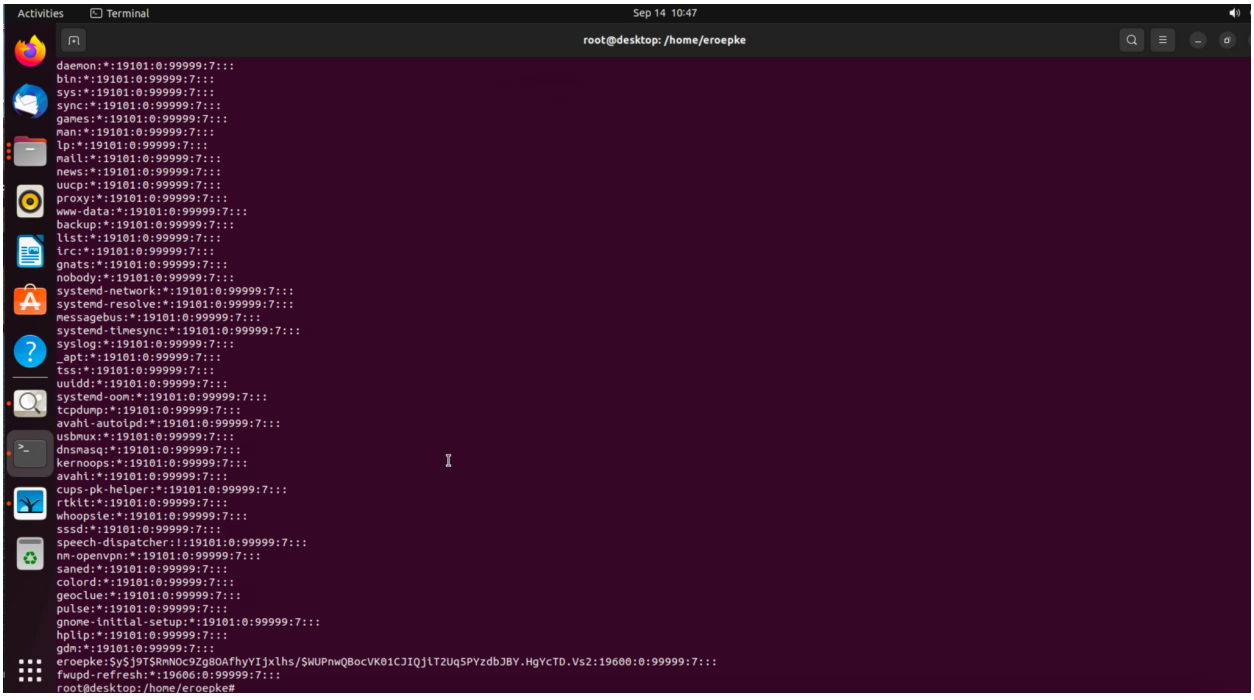
# Lab 03 Template - Ethan Roepke

[Don’t forget to follow these lab report instructions.]

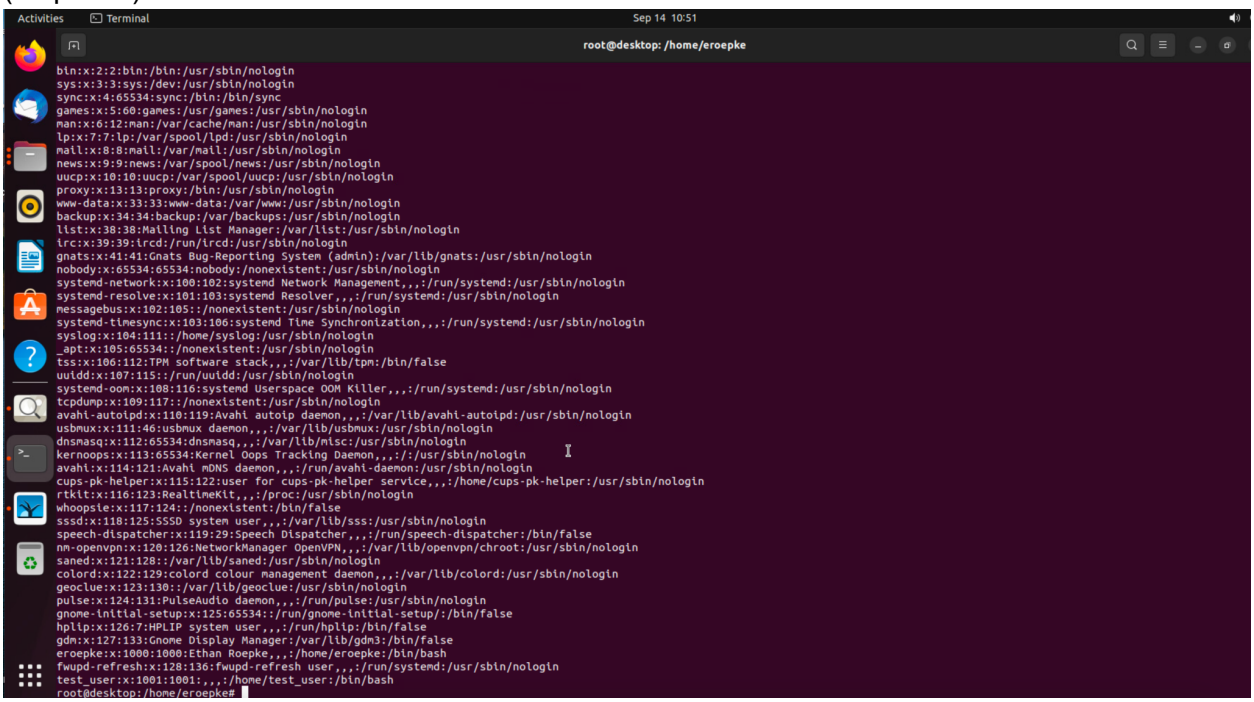
1. **Screenshot of `passwd` and `shadow` with description/notation of fields** (10 points)



The /etc/passwd is a text file with information for al user accounts. It gives information such as User ID, group ID, home directory, and default shell.
The /etc/shadow file stores encrypted user passwords. Only the root user will be able to view to prevent from malicious actors.

2. **Screenshot of `passwd` and shadow in middle of user account creation** (10 points)




3. **Screenshot of new user's home directory contents (`ls -la`) and the output of the environment variables (`echo $USER $SHELL`)**

(5 points)

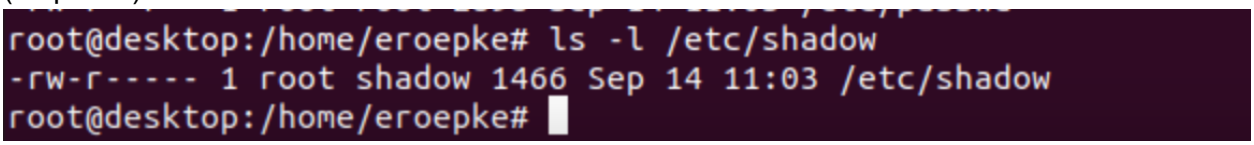

4. **Summarize the Key Differences between nologin and a locked password**
   (5 points)
   Nologin will prevent the user from logging in entirely and locked password will allow the user to login but will not allow them to change the password. A nologin would be used if you dont want a user to gain access to the system anymore while a locked password would be used if you want to prevent the user from changing the password from something else that you want to know.
5. **Description of the effect of each of the (5) `chmod` commands**
   (10 points)

**chmod 777 *filename*** -(-rwxrwxrwx) each number corresponds to user,group,and others. 7 gives access to read,write, and execute. 6 would gives access to read and write. 5 gives access to read and execute. 4 gives access to read. 3 access to write and execute. 2 access to write. 1 execute. 0 access to nothing.
**chmod 700 *filename*** -(-rwx- - - - - -) user has access to read write and execute while group and others have no access.
**chmod u=rw *filename*** - letter before = indicates who it is(u,g,o). This is telling us user gets access to read and write but not execute. This will replace old access to the new access(old: ---e new:-rw-)
**chmod go+x *filename*** - letters before + indicated who it is(u,g,o). Here we are adding access to execute to group and others.
**Chmod a+w filename** - a represents all so user,group,others and added access to execute.

6. **<u>Organized</u> description of directory permissions and how affects contents**
   (10 points)

The permissions determine who can read, write, and execute a file in the directory.
It as well determine who can change the permissions on the directory. Read permission on a directory gives you the ability to read the contents on the file. Write permissions allow you append, remove and rename a file. Execute permission allows you to have access files.

7. **Screenshot and description of `/etc/shadow` file - who can r/w/x and why it's set this way.**
   (10 points)



It is set up this way becasue shadow contains password hashes and we do not want to give access to others to see at all and allow a group to see. Only the user should be able to read and write. You dont want to allow others to gain access and do attacks.

8. **Meanings of `dig` queries**
   (10 points)

| Query | What does the query result mean? |
|---|---|
| `dig -t mx iastate.edu` | Retrieve DNS records and tells mail how to route mail to domain |
| `dig -t ns iastate.edu` | Map a domain name to list of DNS servers for that domain |
| `dig -t soa iastate.edu` | Stores important information about a domain |
| `dig -t aaaa iastate.edu` | Domains are assigned the IPv6 address for a destination |
| `dig -t any iastate.edu` | Shows all domain records and assigned to any |

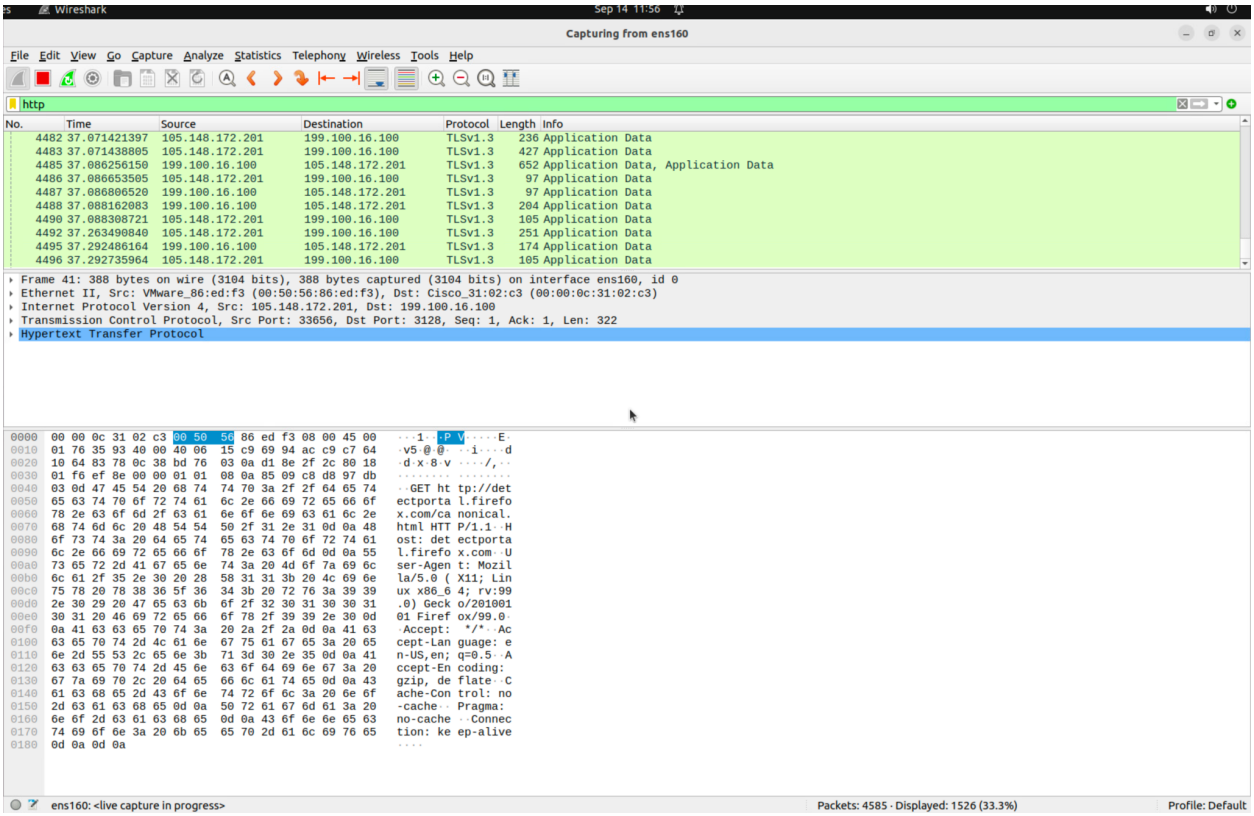
9. **Screenshot of the (2) netstat outputs**
   (10 points)

```
[1]+  Stopped                 sudo netcat -l 22
root@desktop:/home/eroepke# netstat -tl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
root@desktop:/home/eroepke# netstat -tln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
root@desktop:/home/eroepke#
```

10. **Complete the netstat flag table**
    (10 points for all 3 correct meanings; 0 points for anything less)

| Flag | Meaning |
|---|---|
| `-t` | Sort by time, newest first |
| `-l` | Show only listening sockets |
| `-n` | Show number addresses instead of determining host,port, or user name |

11. **Screenshot of the captured `http` traffic using Wireshark**
    (5 points)




## 12. Screenshot of the captured icmp traffic using `tcpdump` (5 points)