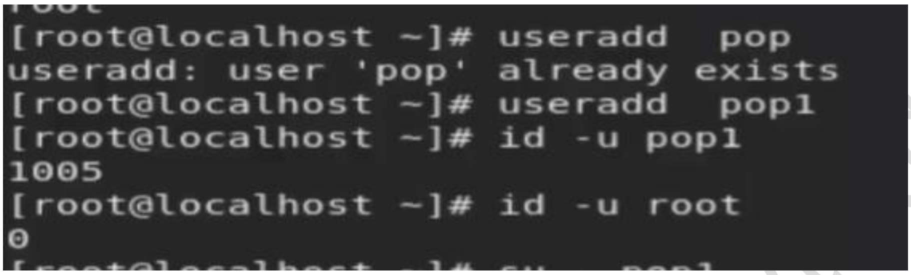
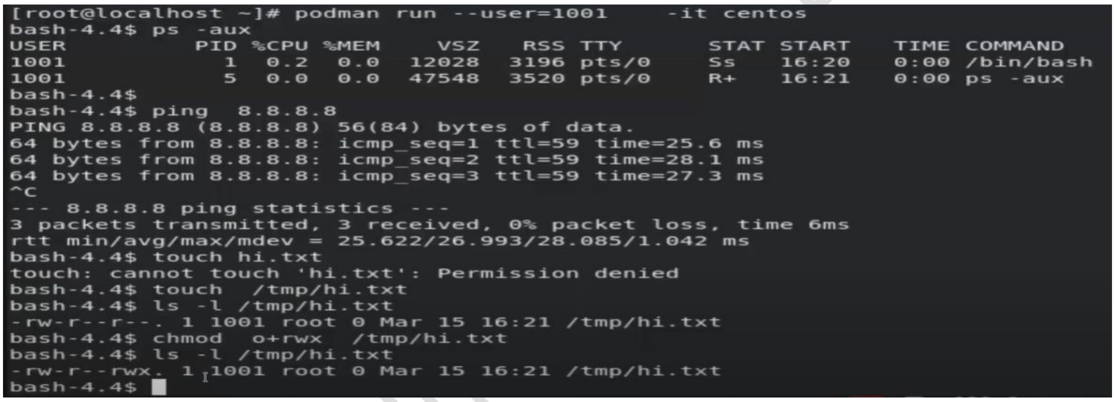
Summary

- Command to create a general user in Linux



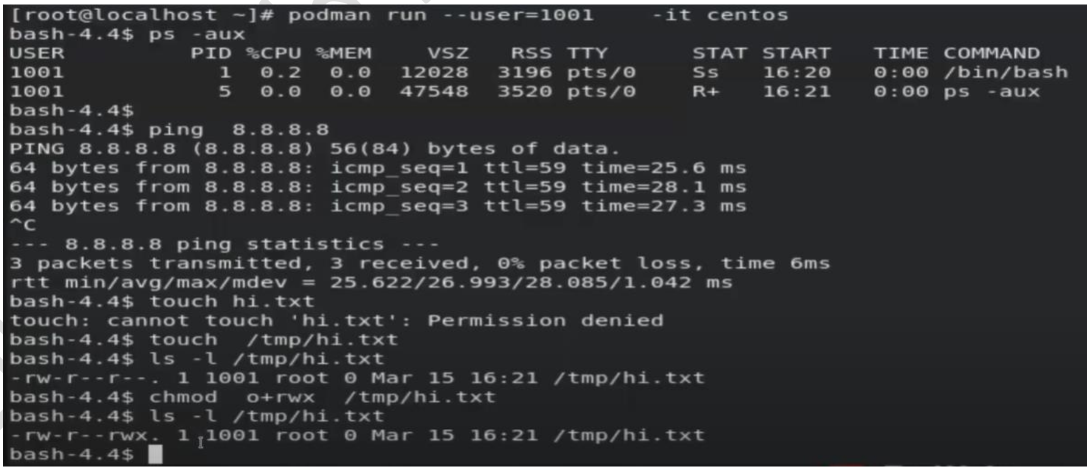
```
root
[root@localhost ~]# useradd  pop
useradd: user 'pop' already exists
[root@localhost ~]# useradd  pop1
[root@localhost ~]# id -u pop1
1005
[root@localhost ~]# id -u root
0
[root@localhost ~]# su  pop1
```

- A general user of Linux has no system-level power



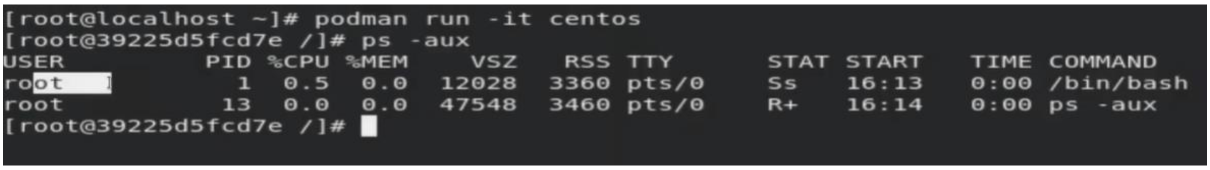
```
[root@localhost ~]# podman run --user=1001    -it centos
bash-4.4$ ps -aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
1001            1  0.2  0.0  12028  3196 pts/0    Ss   16:20   0:00 /bin/bash
1001            5  0.0  0.0  47548  3520 pts/0    R+   16:21   0:00 ps -aux
bash-4.4$
bash-4.4$ ping  8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=59 time=25.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=59 time=28.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=59 time=27.3 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 25.622/26.993/28.085/1.042 ms
bash-4.4$ touch hi.txt
touch: cannot touch 'hi.txt': Permission denied
bash-4.4$ touch  /tmp/hi.txt
bash-4.4$ ls -l /tmp/hi.txt
-rw-r--r--. 1 1001 root 0 Mar 15 16:21 /tmp/hi.txt
bash-4.4$ chmod  o+rwx  /tmp/hi.txt
bash-4.4$ ls -l /tmp/hi.txt
-rw-r--rwx. 1 1001 root 0 Mar 15 16:21 /tmp/hi.txt
bash-4.4$
```

- Command to run a container with general user power

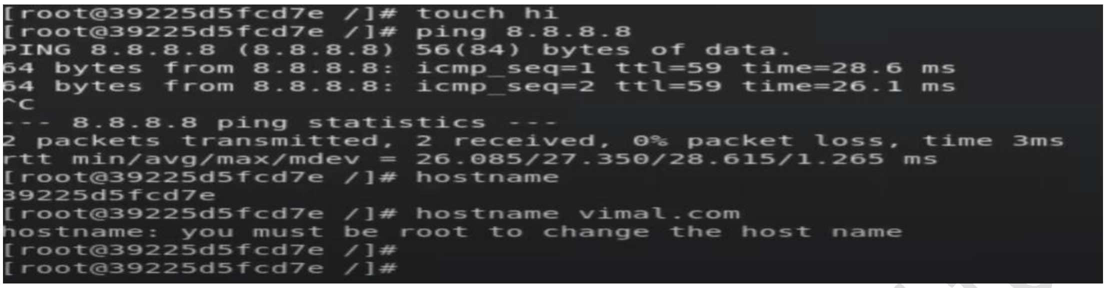


```
[root@localhost ~]# podman run --user=1001    -it centos
bash-4.4$ ps -aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
1001            1  0.2  0.0  12028  3196 pts/0    Ss   16:20   0:00 /bin/bash
1001            5  0.0  0.0  47548  3520 pts/0    R+   16:21   0:00 ps -aux
bash-4.4$
bash-4.4$ ping  8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=59 time=25.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=59 time=28.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=59 time=27.3 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 25.622/26.993/28.085/1.042 ms
bash-4.4$ touch hi.txt
touch: cannot touch 'hi.txt': Permission denied
bash-4.4$ touch  /tmp/hi.txt
bash-4.4$ ls -l /tmp/hi.txt
-rw-r--r--. 1 1001 root 0 Mar 15 16:21 /tmp/hi.txt
bash-4.4$ chmod  o+rwx  /tmp/hi.txt
bash-4.4$ ls -l /tmp/hi.txt
-rw-r--rwx. 1 1001 root 0 Mar 15 16:21 /tmp/hi.txt
bash-4.4$
```

- A good practice is always to run the app with a general user
- Capabilities in Linux allows user to access/restrict certain parts of the system without root privileges
- Root user in Linux operating system has all the capabilities
- Practical:- Checking capabilities of container



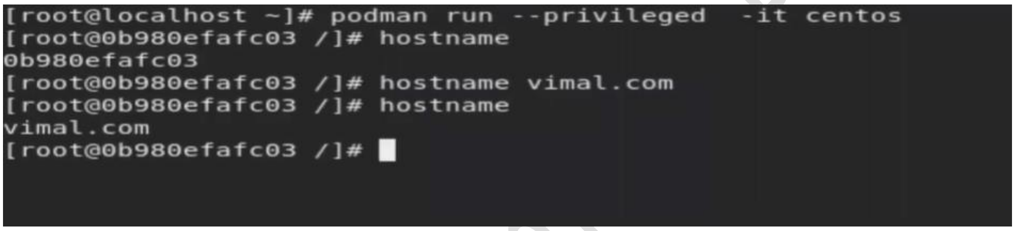
```
[root@localhost ~]# podman run -it centos
[root@39225d5fcd7e /]# ps -aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.5  0.0  12028  3360 pts/0    Ss   16:13   0:00 /bin/bash
root          13  0.0  0.0  47548  3460 pts/0    R+   16:14   0:00 ps -aux
[root@39225d5fcd7e /]#
```



```
[root@39225d5fcd7e /]# touch hi
[root@39225d5fcd7e /]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=59 time=28.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=59 time=26.1 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3ms
rtt min/avg/max/mdev = 26.085/27.350/28.615/1.265 ms
[root@39225d5fcd7e /]# hostname
39225d5fcd7e
[root@39225d5fcd7e /]# hostname vimal.com
hostname: you must be root to change the host name
[root@39225d5fcd7e /]#
[root@39225d5fcd7e /]#
```

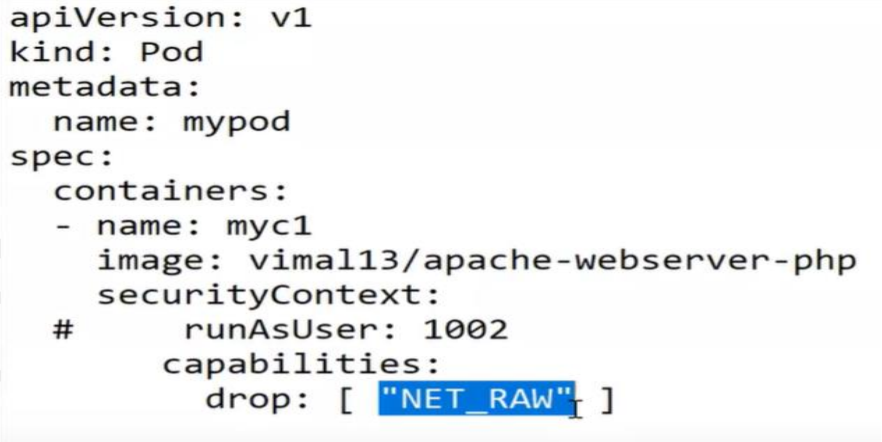
Even though the container is running with a root user it cannot change the hostname

- Privileged is a way to give all the power to the container



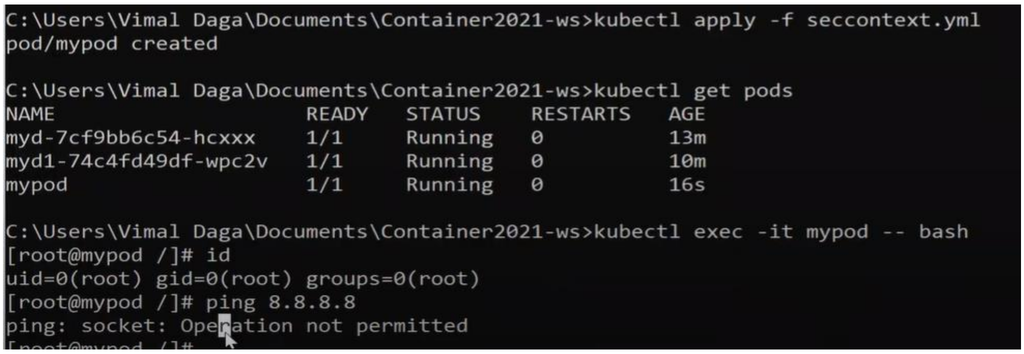
```
[root@localhost ~]# podman run --privileged  -it centos
[root@0b980efafc03 /]# hostname
0b980efafc03
[root@0b980efafc03 /]# hostname vimal.com
[root@0b980efafc03 /]# hostname
vimal.com
[root@0b980efafc03 /]#
```

- Practical:- Removing capability from a pod
  - Manifest file for pod



```
apiVersion: v1
kind: Pod
metadata:
  name: mypod
spec:
  containers:
  - name: myc1
    image: vimal13/apache-webserver-php
    securityContext:
  #     runAsUser: 1002
       capabilities:
         drop: [ "NET_RAW" ]
```

  - Creating a pod with capabilities



```
C:\Users\Vimal Daga\Documents\Container2021-ws>kubectl apply -f seccontext.yml
pod/mypod created

C:\Users\Vimal Daga\Documents\Container2021-ws>kubectl get pods
NAME                     READY   STATUS    RESTARTS   AGE
myd-7cf9bb6c54-hcxxx     1/1     Running   0          13m
myd1-74c4fd49df-wpc2v    1/1     Running   0          10m
mypod                    1/1     Running   0          16s

C:\Users\Vimal Daga\Documents\Container2021-ws>kubectl exec -it mypod -- bash
[root@mypod /]# id
uid=0(root) gid=0(root) groups=0(root)
[root@mypod /]# ping 8.8.8.8
ping: socket: Operation not permitted
[root@mypod /]#
```