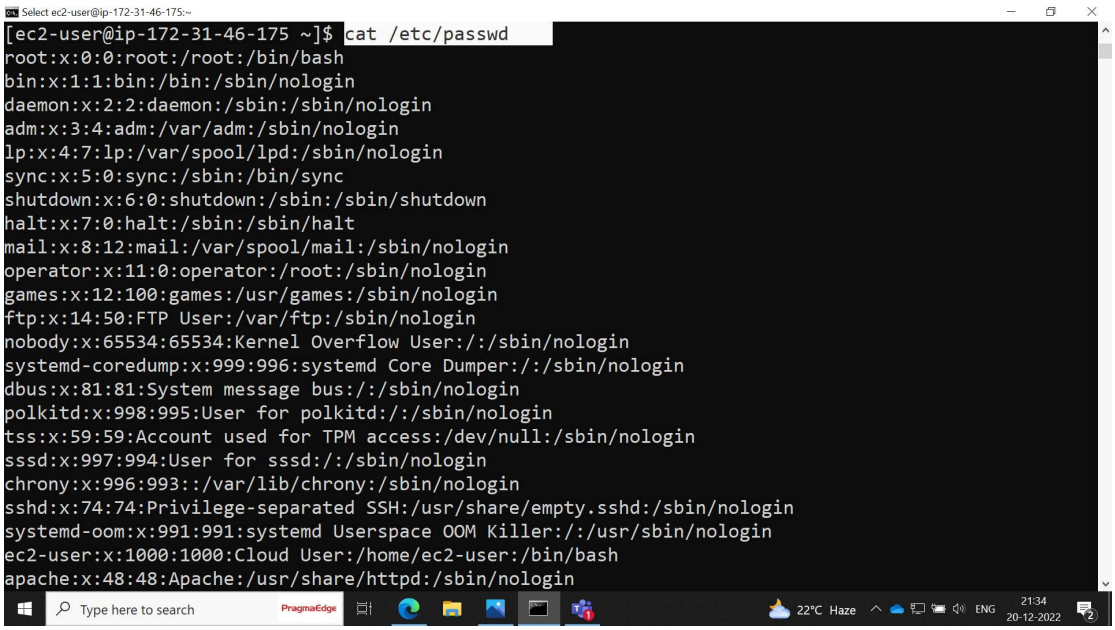
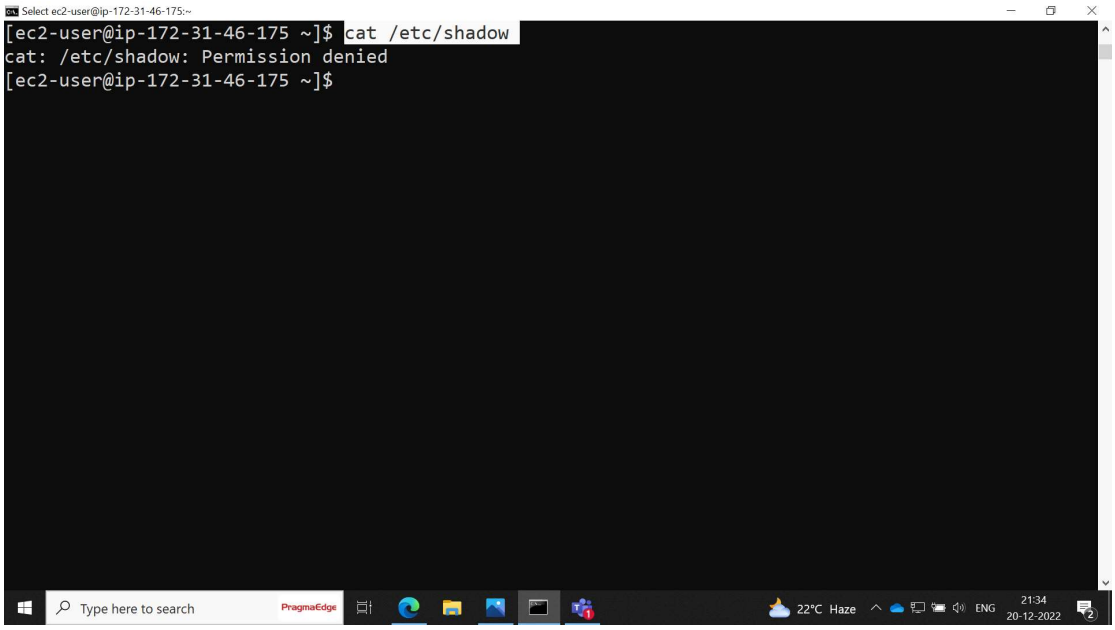
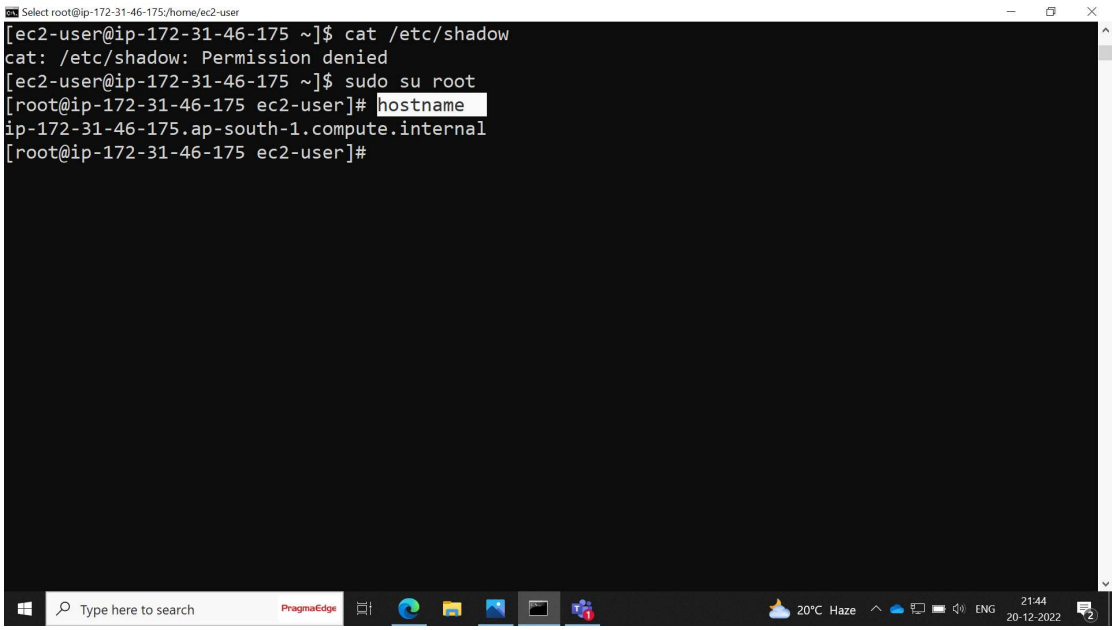
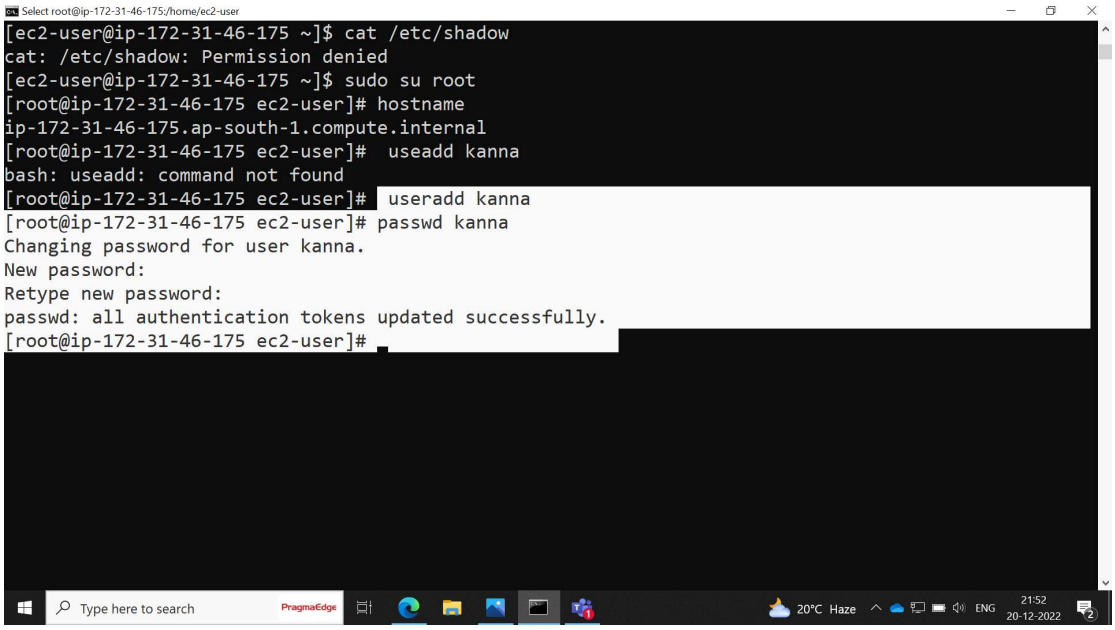
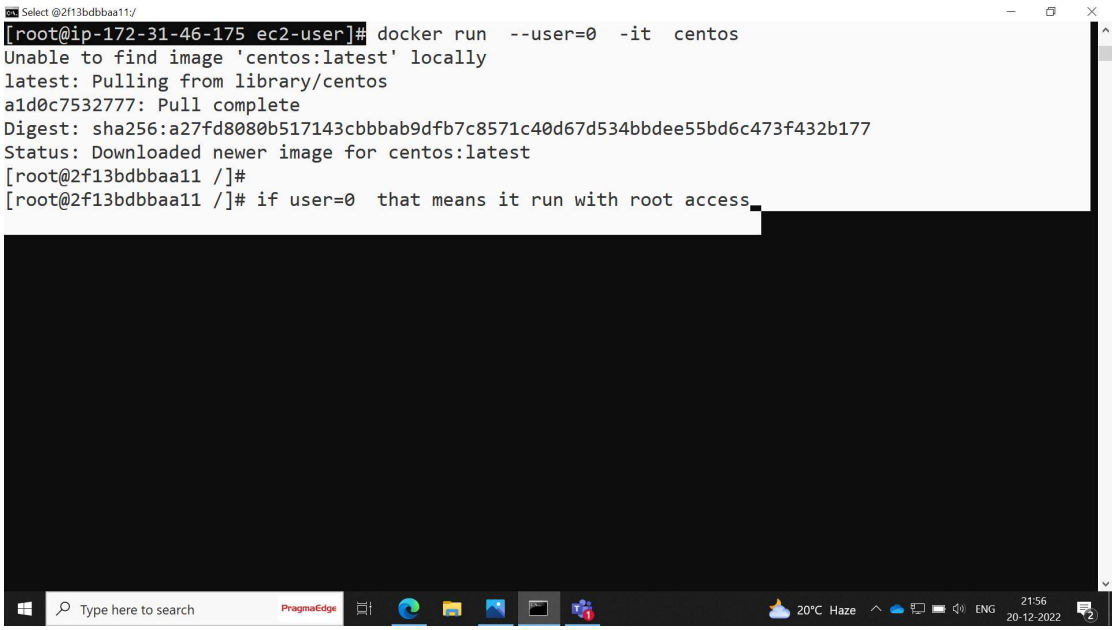
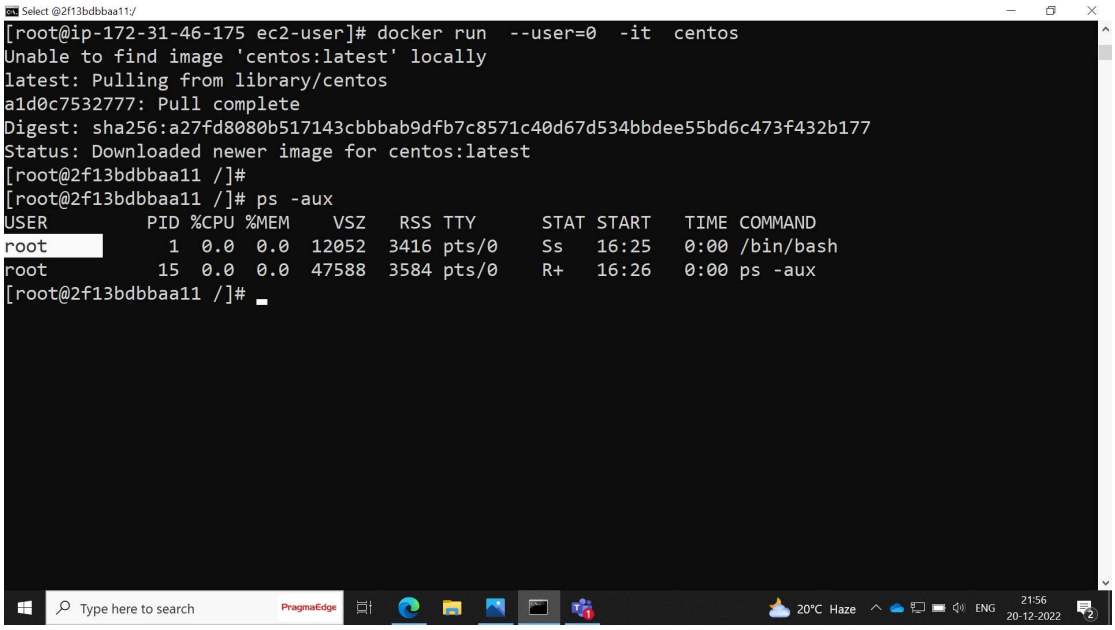

Select ec2-user@ip-172-31-46-175:~
[ec2-user@ip-172-31-46-175 ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
systemd-coredump:x:999:996:systemd Core Dumper:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:998:995:User for polkitd:/:/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
sssd:x:997:994:User for sssd:/:/sbin/nologin
chrony:x:996:993::/var/lib/chrony:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
systemd-oom:x:991:991:systemd Userspace OOM Killer:/:/usr/sbin/nologin
ec2-user:x:1000:1000:Cloud User:/home/ec2-user:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
Type here to search
PragmaEdge
22°C Haze
ENG
21:34
20-12-2022

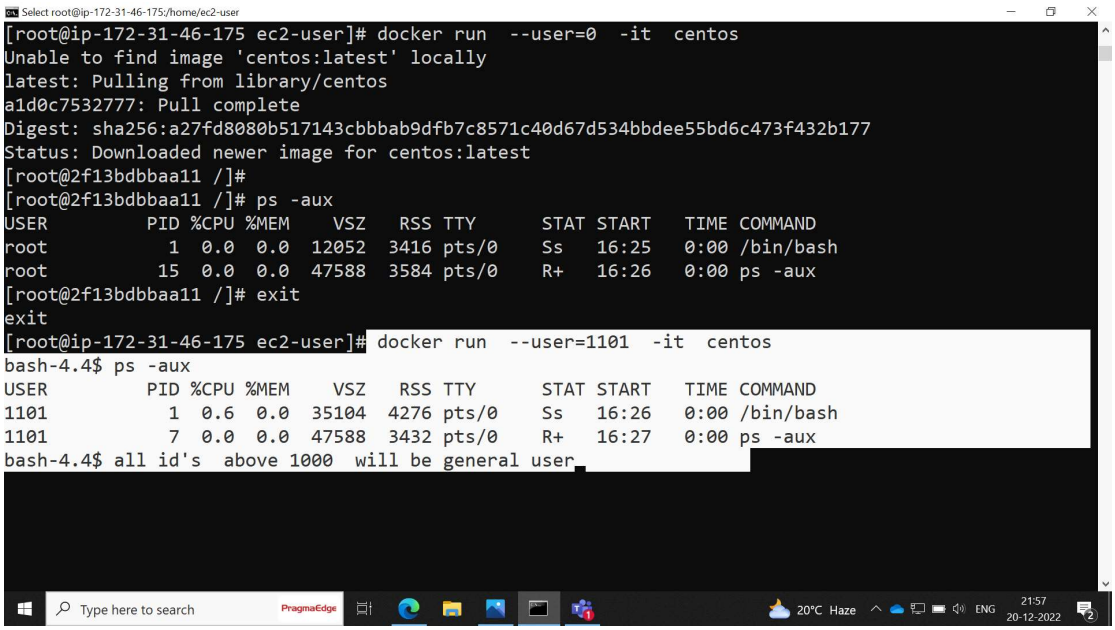

Select ec2-user@ip-172-31-46-175:~
[ec2-user@ip-172-31-46-175 ~]$ cat /etc/shadow
cat: /etc/shadow: Permission denied
[ec2-user@ip-172-31-46-175 ~]$
Type here to search
PragmaEdge
22°C Haze
ENG
21:34
20-12-2022

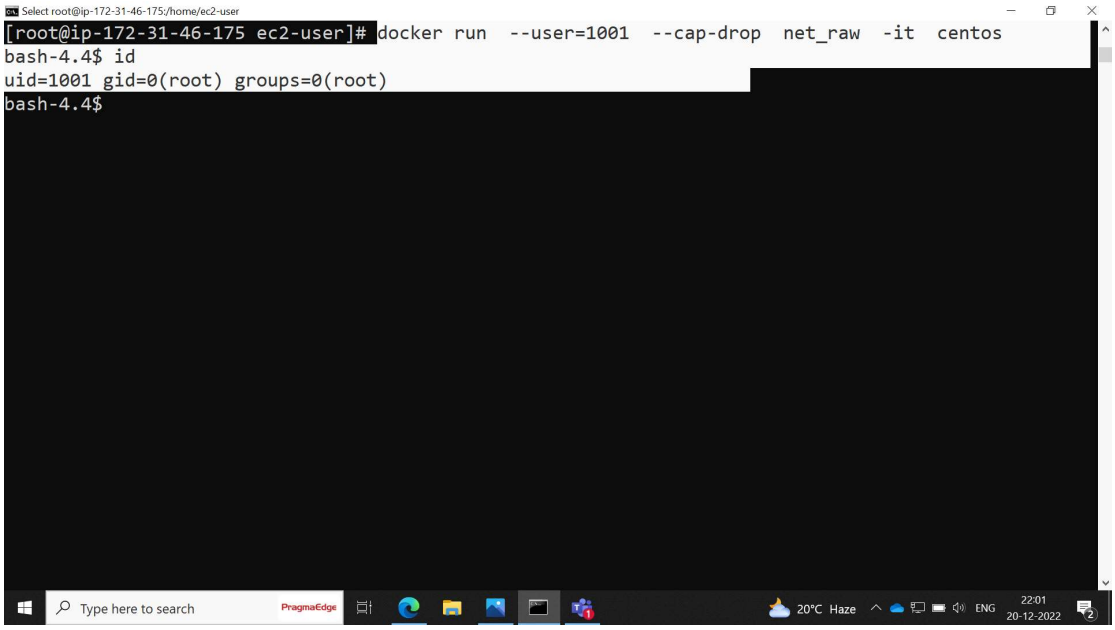

Select root@ip-172-31-46-175:/home/ec2-user
[ec2-user@ip-172-31-46-175 ~]$ cat /etc/shadow
cat: /etc/shadow: Permission denied
[ec2-user@ip-172-31-46-175 ~]$ sudo su root
[root@ip-172-31-46-175 ec2-user]# hostname
ip-172-31-46-175.ap-south-1.compute.internal
[root@ip-172-31-46-175 ec2-user]#
Type here to search
PragmaEdge
20°C Haze
ENG
21:44
20-12-2022

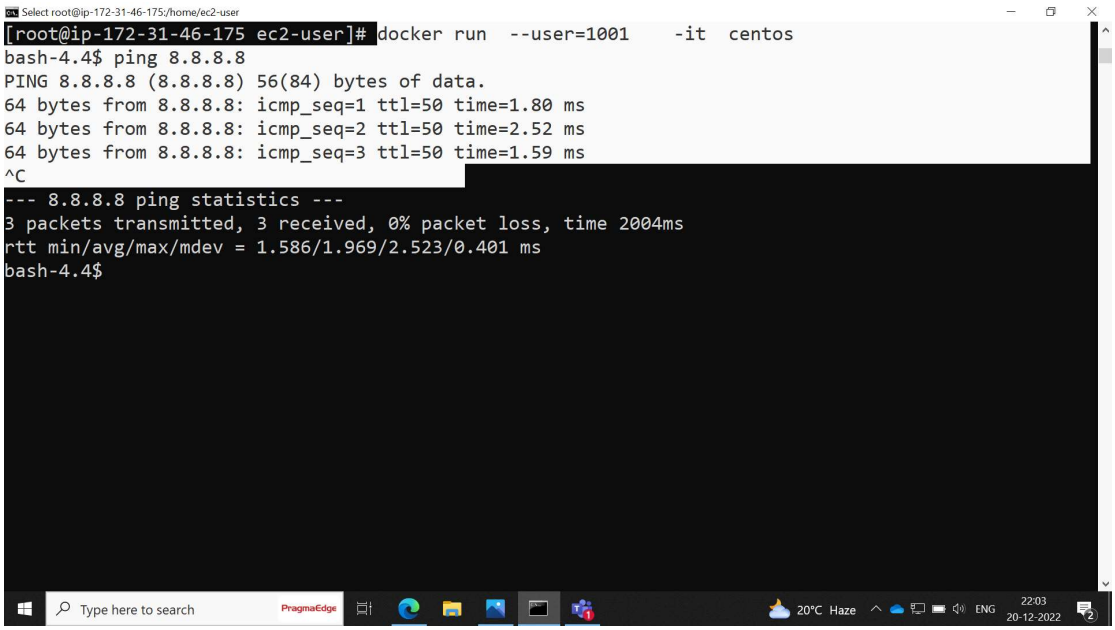

Select root@ip-172-31-46-175:/home/ec2-user
[ec2-user@ip-172-31-46-175 ~]$ cat /etc/shadow
cat: /etc/shadow: Permission denied
[ec2-user@ip-172-31-46-175 ~]$ sudo su root
[root@ip-172-31-46-175 ec2-user]# hostname
ip-172-31-46-175.ap-south-1.compute.internal
[root@ip-172-31-46-175 ec2-user]# useadd kanna
bash: useadd: command not found
[root@ip-172-31-46-175 ec2-user]# useradd kanna
[root@ip-172-31-46-175 ec2-user]# passwd kanna
Changing password for user kanna.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@ip-172-31-46-175 ec2-user]#
Type here to search
PragmaEdge
20°C Haze
ENG
21:52
20-12-2022

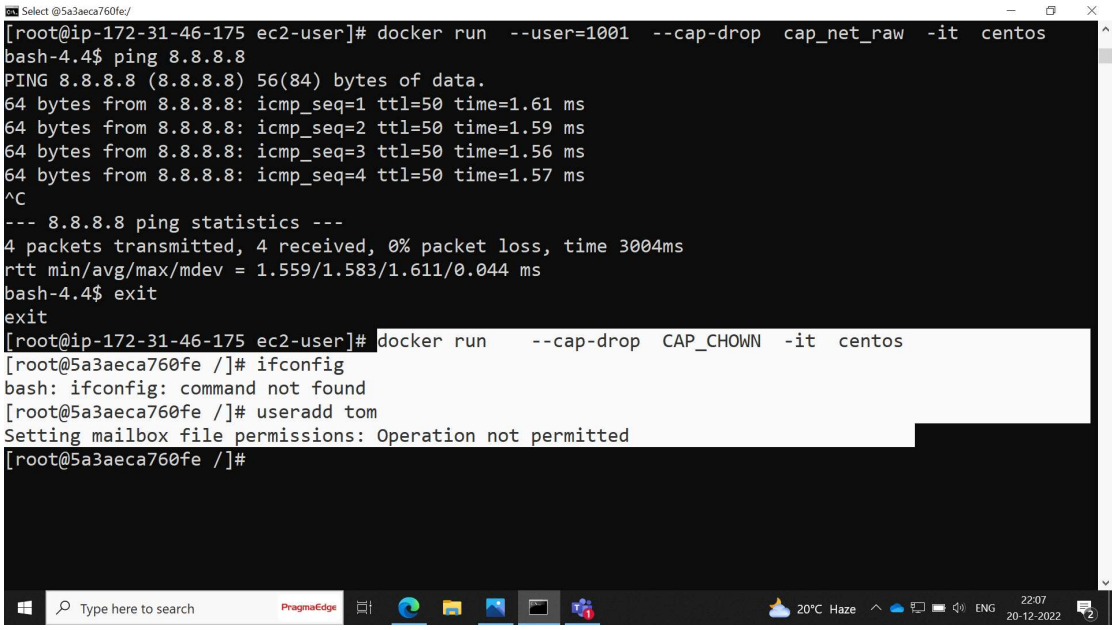

Select @2f13bdbbaa11:/
[root@ip-172-31-46-175 ec2-user]# docker run --user=0 -it centos
Unable to find image 'centos:latest' locally
latest: Pulling from library/centos
a1d0c7532777: Pull complete
Digest: sha256:a27fd8080b517143cbbbab9dfb7c8571c40d67d534bbdee55bd6c473f432b177
Status: Downloaded newer image for centos:latest
[root@2f13bdbbaa11 /]#
[root@2f13bdbbaa11 /]# if user=0 that means it run with root access
Type here to search
PragmaEdge
20°C Haze
ENG
21:56
20-12-2022

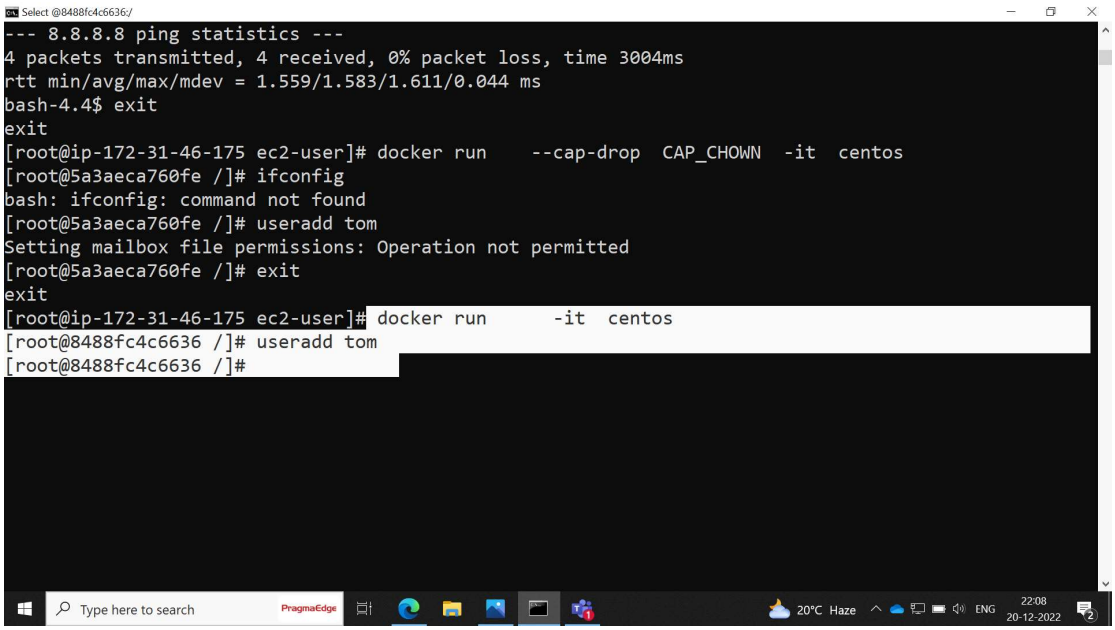

Select @2f13bdbbaa11:/
[root@ip-172-31-46-175 ec2-user]# docker run --user=0 -it centos
Unable to find image 'centos:latest' locally
latest: Pulling from library/centos
a1d0c7532777: Pull complete
Digest: sha256:a27fd8080b517143cbbbab9dfb7c8571c40d67d534bbdee55bd6c473f432b177
Status: Downloaded newer image for centos:latest
[root@2f13bdbbaa11 /]#
[root@2f13bdbbaa11 /]# ps -aux
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.0 0.0 12052 3416 pts/0 Ss 16:25 0:00 /bin/bash
root 15 0.0 0.0 47588 3584 pts/0 R+ 16:26 0:00 ps -aux
[root@2f13bdbbaa11 /]#
Type here to search
PragmaEdge
20°C Haze
ENG
21:56
20-12-2022

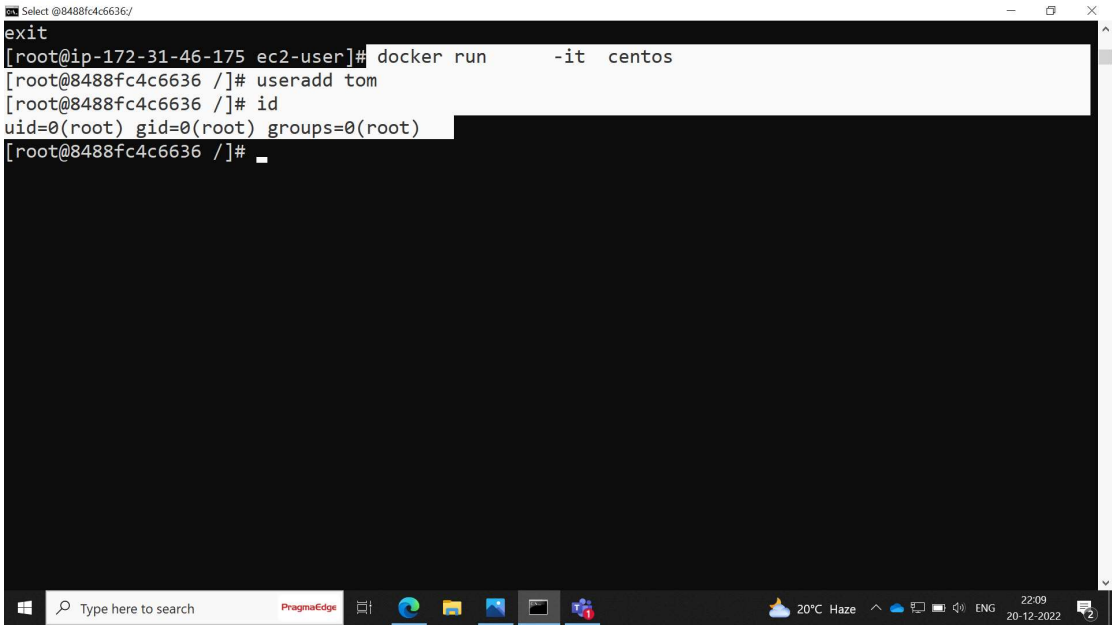

Select root@ip-172-31-46-175:/home/ec2-user
[root@ip-172-31-46-175 ec2-user]# docker run --user=0 -it centos
Unable to find image 'centos:latest' locally
latest: Pulling from library/centos
a1d0c7532777: Pull complete
Digest: sha256:a27fd8080b517143cbbbab9dfb7c8571c40d67d534bbdee55bd6c473f432b177
Status: Downloaded newer image for centos:latest
[root@2f13bdbbaa11 /]#
[root@2f13bdbbaa11 /]# ps -aux
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.0 0.0 12052 3416 pts/0 Ss 16:25 0:00 /bin/bash
root 15 0.0 0.0 47588 3584 pts/0 R+ 16:26 0:00 ps -aux
[root@2f13bdbbaa11 /]# exit
exit
[root@ip-172-31-46-175 ec2-user]# docker run --user=1101 -it centos
bash-4.4$ ps -aux
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
1101 1 0.6 0.0 35104 4276 pts/0 Ss 16:26 0:00 /bin/bash
1101 7 0.0 0.0 47588 3432 pts/0 R+ 16:27 0:00 ps -aux
bash-4.4$ all id's above 1000 will be general user
Type here to search
PragmaEdge
20°C Haze
ENG
21:57
20-12-2022

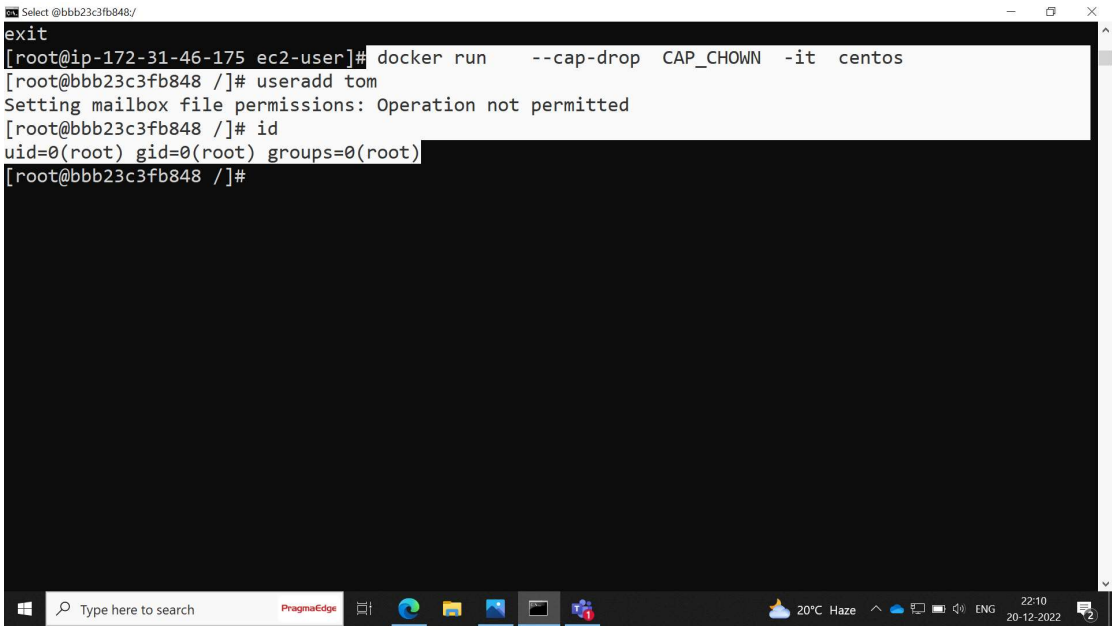

Select root@ip-172-31-46-175:/home/ec2-user
[root@ip-172-31-46-175 ec2-user]# docker run --user=1001 --cap-drop net_raw -it centos
bash-4.4$ id
uid=1001 gid=0(root) groups=0(root)
bash-4.4$
Type here to search
PragmaEdge
20°C Haze
ENG
22:01
20-12-2022

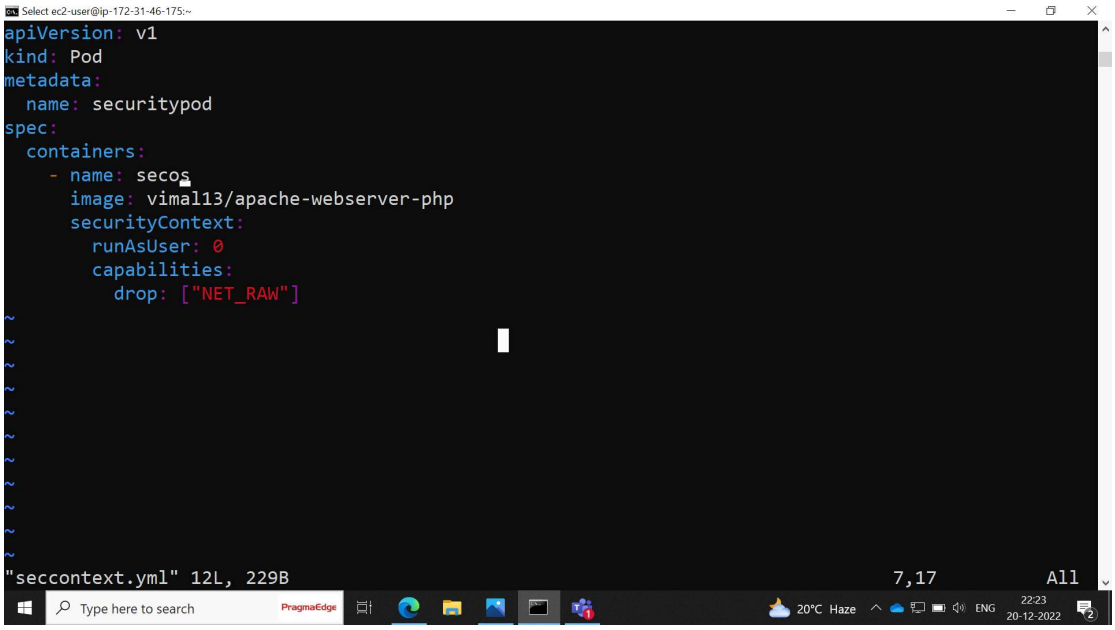

Select root@ip-172-31-46-175:/home/ec2-user
[root@ip-172-31-46-175 ec2-user]# docker run --user=1001 -it centos
bash-4.4$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=50 time=1.80 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=50 time=2.52 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=50 time=1.59 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.586/1.969/2.523/0.401 ms
bash-4.4$
Type here to search
PragmaEdge
20°C Haze
ENG
22:03
20-12-2022

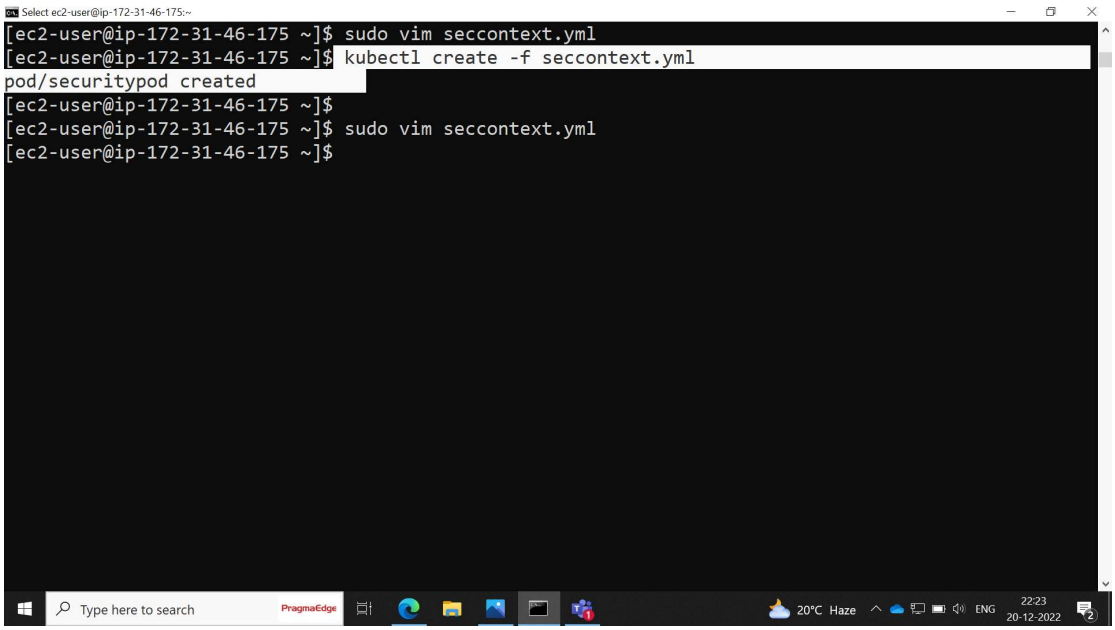

Select @5a3aeca760fe:/
[root@ip-172-31-46-175 ec2-user]# docker run --user=1001 --cap-drop cap_net_raw -it centos
bash-4.4$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=50 time=1.61 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=50 time=1.59 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=50 time=1.56 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=50 time=1.57 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.559/1.583/1.611/0.044 ms
bash-4.4$ exit
exit
[root@ip-172-31-46-175 ec2-user]# docker run --cap-drop CAP_CHOWN -it centos
[root@5a3aeca760fe /]# ifconfig
bash: ifconfig: command not found
[root@5a3aeca760fe /]# useradd tom
Setting mailbox file permissions: Operation not permitted
[root@5a3aeca760fe /]#
Type here to search
PragmaEdge
20°C Haze
ENG
22:07
20-12-2022


Select @8488fc4c6636:/
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.559/1.583/1.611/0.044 ms
bash-4.4$ exit
exit
[root@ip-172-31-46-175 ec2-user]# docker run --cap-drop CAP_CHOWN -it centos
[root@5a3aeca760fe /]# ifconfig
bash: ifconfig: command not found
[root@5a3aeca760fe /]# useradd tom
Setting mailbox file permissions: Operation not permitted
[root@5a3aeca760fe /]# exit
exit
[root@ip-172-31-46-175 ec2-user]# docker run -it centos
[root@8488fc4c6636 /]# useradd tom
[root@8488fc4c6636 /]#
Type here to search
PragmaEdge
20°C Haze
ENG
22:08
20-12-2022


Select @8488fc4c6636:/
exit
[root@ip-172-31-46-175 ec2-user]# docker run -it centos
[root@8488fc4c6636 /]# useradd tom
[root@8488fc4c6636 /]# id
uid=0(root) gid=0(root) groups=0(root)
[root@8488fc4c6636 /]#
Type here to search
PragmaEdge
20°C Haze
ENG
22:09
20-12-2022


Select @bbb23c3fb848:/
exit
[root@ip-172-31-46-175 ec2-user]# docker run --cap-drop CAP_CHOWN -it centos
[root@bbb23c3fb848 /]# useradd tom
Setting mailbox file permissions: Operation not permitted
[root@bbb23c3fb848 /]# id
uid=0(root) gid=0(root) groups=0(root)
[root@bbb23c3fb848 /]#
Type here to search
PragmaEdge
20°C Haze
ENG
22:10
20-12-2022


Select ec2-user@ip-172-31-46-175:~
apiVersion: v1
kind: Pod
metadata:
name: securitypod
spec:
containers:
- name: secos
image: vimal13/apache-webserver-php
securityContext:
runAsUser: 0
capabilities:
drop: ["NET_RAW"]
"seccontext.yml" 12L, 229B
7,17
All
Type here to search
PragmaEdge
20°C Haze
ENG
22:23
20-12-2022


Select ec2-user@ip-172-31-46-175:~
[ec2-user@ip-172-31-46-175 ~]$ sudo vim seccontext.yml
[ec2-user@ip-172-31-46-175 ~]$ kubectl create -f seccontext.yml
pod/securitypod created
[ec2-user@ip-172-31-46-175 ~]$
[ec2-user@ip-172-31-46-175 ~]$ sudo vim seccontext.yml
[ec2-user@ip-172-31-46-175 ~]$
Type here to search
PragmaEdge
20°C Haze
ENG
22:23
20-12-2022