

## LAB 2 - REPORT

Justin Kaipada - 100590167

February 7, 2020

## Task #1: Experiencing Capabilities

By default ping was a **Set-UID** program

```
justin@justin-Precision-3520 11:22:57 ~  
$ ls -l /bin/ping  
-rwsr-xr-x 1 root root 64424 Jun 28 2019 /bin/ping
```

After changing

```
root@justin-Precision-3520:/home/justin# ls -l /bin/ping  
-rwxr-xr-x 1 root root 64424 Jun 28 2019 /bin/ping
```

Before changing ping

```
justin@justin-Precision-3520 11:22:45 ~  
$ ping www.google.com  
PING www.google.com (172.217.1.4) 56(84) bytes of data.  
64 bytes from yyz10s14-in-f4.1e100.net (172.217.1.4): icmp_seq=1 ttl=54 time=9.98 ms  
64 bytes from yyz10s14-in-f4.1e100.net (172.217.1.4): icmp_seq=2 ttl=54 time=10.1 ms  
64 bytes from yyz10s14-in-f4.1e100.net (172.217.1.4): icmp_seq=3 ttl=54 time=12.8 ms  
64 bytes from yyz10s14-in-f4.1e100.net (172.217.1.4): icmp_seq=4 ttl=54 time=7.64 ms  
64 bytes from yyz10s14-in-f4.1e100.net (172.217.1.4): icmp_seq=5 ttl=54 time=12.4 ms  
^C  
--- www.google.com ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4004ms  
rtt min/avg/max/mdev = 7.648/10.612/12.819/1.875 ms
```

After changing ping to **non-Set-UID** program

```
justin@justin-Precision-3520 11:35:52 ~  
$ ping google.com  
ping: socket: Operation not permitted
```

After giving `cap_net_raw` capability

```
justin@justin-Precision-3520 11:37:01 ~  
$ ping google.com  
PING google.com (172.217.1.174) 56(84) bytes of data.  
64 bytes from yyz10s04-in-f14.1e100.net (172.217.1.174): icmp_seq=1 ttl=54 time=6.25 ms  
64 bytes from yyz10s04-in-f14.1e100.net (172.217.1.174): icmp_seq=2 ttl=54 time=6.04 ms  
64 bytes from yyz10s04-in-f14.1e100.net (172.217.1.174): icmp_seq=3 ttl=54 time=6.54 ms  
^C  
--- google.com ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2003ms  
rtt min/avg/max/mdev = 6.049/6.283/6.546/0.223 ms
```

## Question 1

```
setcap cap_fowner,cap_chown,cap_dac_override+ep /usr/bin/passwd
```

## Question 2

**capdacreadsearch**

**capdacoverride**

**capchown**

**capsetuid**

**capkill**

**capnetraw**