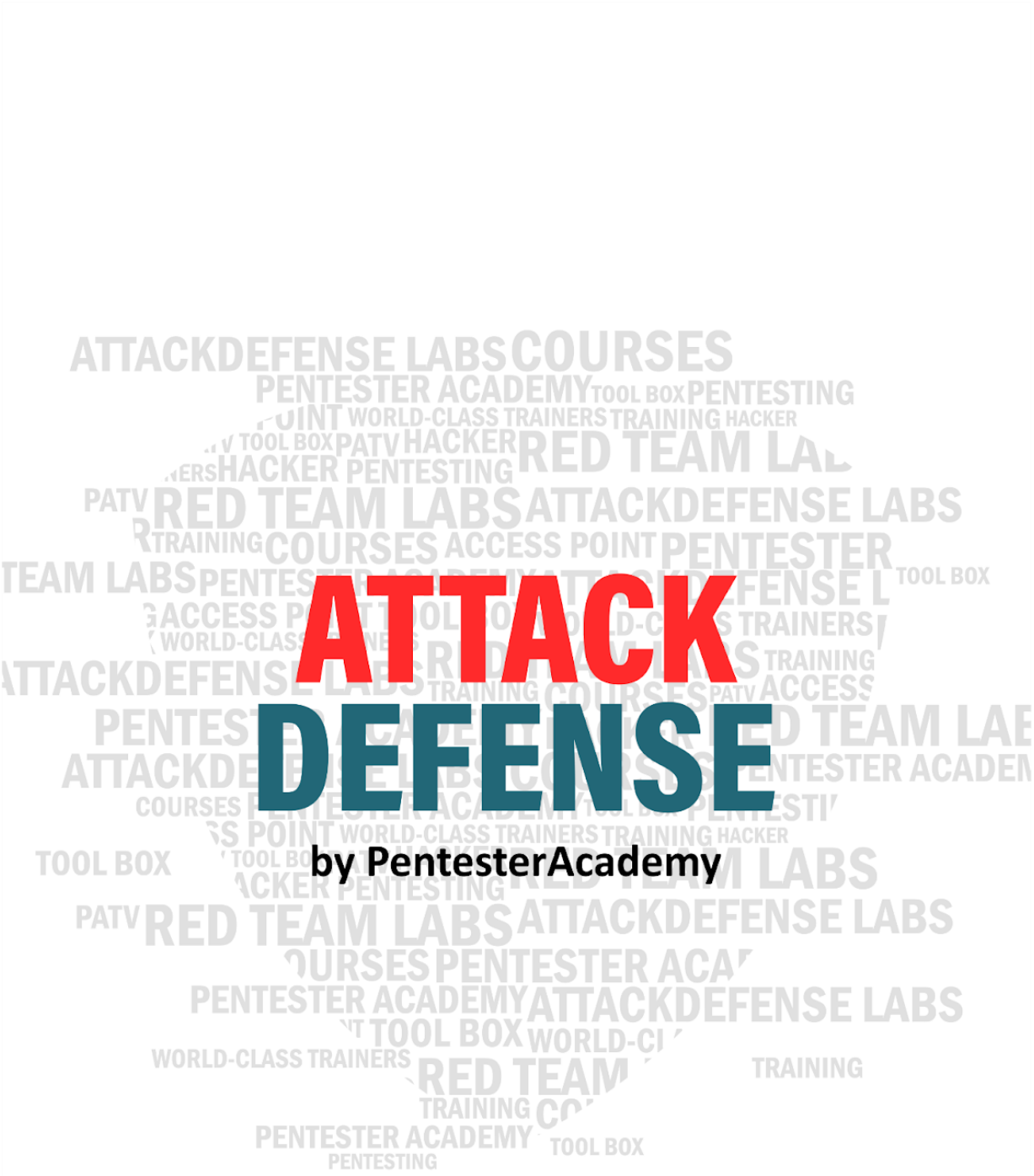
ATTACK
DEFENSE
by PentesterAcademy

Name	Linux Capabilities
URL	https://attackdefense.com/challengedetails?cid=1823
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: Learn about Linux Capabilities using an example of tcpdump command.

Solution:

Check the connected interfaces of the machine.

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 86225sec preferred_lft 14225sec
    inet6 fe80::5054:ff:fe12:3456/64 scope link
       valid_lft forever preferred_lft forever
student@localhost:~$
```

Run tcpdump on interface ens3

Command: tcpdump -i ens3

```
student@localhost:~$ tcpdump -i ens3
tcpdump: ens3: You don't have permission to capture on that device
(socket: Operation not permitted)
student@localhost:~$
```

The user student doesn't have the necessary permissions to run tcpdump on the ens3 interface. Locate the tcpdump binary.

Command: whereis tcpdump

```
student@localhost:~$ whereis tcpdump
tcpdump: /usr/sbin/tcpdump /usr/share/man/man8/tcpdump.8.gz
student@localhost:~$
```

Add CAP_NET_RAW capability to the permitted set of tcpdump binary.

Command: sudo setcap 'cap_net_raw+p' /usr/sbin/tcpdump

```
student@localhost:~$ sudo setcap 'cap_net_raw+p' /usr/sbin/tcpdump
```

Again, run tcpdump on interface ens3

Command: tcpdump -i ens3

```
student@localhost:~$ tcpdump -i ens3
tcpdump: ens3: You don't have permission to capture on that device
(socket: Operation not permitted)
student@localhost:~$
```

The tcpdump is not running because unlike the ping command, it is not "Capability-aware" like ping. So, it can't bring CAP_NET_RAW capability to the effective set from the permitted set. Hence, it is not able to capture the traffic.

To fix this, add CAP_NET_RAW capability to both effective and permitted sets of tcpdump binary.

Command: sudo setcap 'cap_net_raw+ep' /usr/sbin/tcpdump

```
student@localhost:~$ sudo setcap 'cap_net_raw+ep' /usr/sbin/tcpdump
```

Again, run tcpdump on interface ens3

Command: tcpdump -i ens3

```
student@localhost:~$ tcpdump -i ens3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
12:10:24.126164 IP 10.0.2.15.ssh > 192.46.213.2.37846: Flags [P.], seq 4046161323:4046161439, ack
12:10:24.126746 IP 192.46.213.2.37846 > 10.0.2.15.ssh: Flags [.], ack 116, win 8760, length 0
12:10:24.127203 IP 10.0.2.15.ssh > 192.46.213.2.37846: Flags [P.], seq 116:232, ack 1, win 62839,
12:10:24.127374 IP 192.46.213.2.37846 > 10.0.2.15.ssh: Flags [.], ack 232, win 8760, length 0
```

This time it was able to capture the traffic.

References:

- Capabilities man page (http://man7.org/linux/man-pages/man7/capabilities.7.html)
- Linux capabilities in practice (https://blog.container-solutions.com/linux-capabilities-in-practice)
- Linux Audit (https://linux-audit.com/linux-capabilities-101/)
- Working with Linux capabilities (https://www.vultr.com/docs/working-with-linux-capabilities)