

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN



MÔN HỌC: PHÂN TÍCH MÃ ĐỘC
BÁO CÁO THỰC HÀNH BÀI 1

Giảng viên: PGS.TS. Đỗ Xuân Chợt

Sinh viên: Hoàng Trung Kiên – B20DCAT098

Hà Nội – 5/2023

Mục lục

1. Tìm hiểu về Linux Capability	3
a, Mục đích.....	3
b, Lý thuyết.....	3
2. Thực hành.....	3
Nhiệm vụ 1: Trải nghiệm Capabilities	4
<i>Nhiệm vụ 1.1: Cho phép người dùng không đặc quyền chạy tcpdump.....</i>	6
Nhiệm vụ 1.2: Chuyển đổi passwd để sử dụng capabilities	6
Nhiệm vụ 2: Điều chỉnh đặc quyền	7
3. Checkwork	10
4. Trả lời câu hỏi	10

1. Tìm hiểu về Linux Capability

a, Mục đích

Mục tiêu học tập của lab này là để sinh viên có được kinh nghiệm trực tiếp về việc sử dụng Linux capabilities để đạt được nguyên tắc của quyền tối thiểu. Lab này dựa trên POSIX 1.e capabilities, được thực hiện trong các phiên bản gần đây của kernel Linux. Hệ thống dựa trên capabilities được đôi khi quảng cáo như là một chiến lược kiểm soát truy cập so với việc sử dụng Access Control Lists (ACLs) hoặc quyền tập tin Unix. Trong thực tế, hệ thống Linux thường sử dụng capabilities để giới hạn đặc quyền của chương trình thay vì để kiểm soát quyền truy cập vào các đối tượng có tên. Lab này tập trung vào việc sử dụng capabilities để giới hạn đặc quyền.

b, Lý thuyết.

Linux Capability là một tập các quyền hạn đặc biệt có thể được cấp cho một tiến trình hoặc tệp. Chúng cung cấp khả năng kiểm soát chi tiết hơn đối với các quyền so với cách phân định root/non-root truyền thống.

Có hai loại Linux Capability:

- Permitted capabilities: Đây là những quyền mà một tiến trình hoặc tệp được phép sử dụng.
- Effective capabilities: Đây là những quyền mà một tiến trình hoặc tệp thực sự đang sử dụng.

Capabilities là một công cụ mạnh mẽ để kiểm soát quyền hạn trong Linux. Chúng có thể được sử dụng để cấp các quyền đặc biệt cho các tiến trình và tệp mà không cần phải biến chúng thành root.

Dưới đây là một số ví dụ về cách sử dụng Linux Capability:

- Một máy chủ web có thể được cấp quyền `CAP_NET_BIND_SERVICE` để nó có thể liên kết với các cổng được ưu tiên.
- Một máy chủ cơ sở dữ liệu có thể được cấp quyền `CAP_SYS_RESOURCE` để nó có thể khóa bộ nhớ.
- Một tệp có thể được cấp quyền `CAP_SETUID` để nó có thể được thực thi dưới dạng người dùng khác.

Capabilities cũng có thể được sử dụng để tạo sandbox cho các tiến trình. Ví dụ, một runtime container có thể sử dụng capabilities để hạn chế quyền hạn của các tiến trình mà nó chạy.

Linux Capabilities là một chủ đề phức tạp, nhưng chúng là một công cụ mạnh mẽ để kiểm soát quyền hạn trong Linux.

2. Thực hành

Khởi động bài lab và nhập mã sinh viên

```
student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Help
good practice to stop labs before transitioning to
new labs or to instructor instances, otherwise there
may be networking name conflicts.

If you wish to restart a lab from scratch, wiping out
all previous data and work in the lab, use:

labtainer <labname> -r
student@ubuntu:~/labtainer/labtainer-student$ labtainer -r capabilities
usage: labtainer [-h] [-q] [-r] [-v] [-k] [-f FIND [FIND ...]] [-d] [-s] [-w]
               [-n CLIENT_COUNT] [-o ONLY_CONTAINER] [-t] [-l]
               [labname]
labtainer: error: unrecognized arguments: capabilities
student@ubuntu:~/labtainer/labtainer-student$ labtainer -r capabilities
latest: Pulling from labtainers/capabilities.capabilities.student
ff94050018be: Pull complete
b49a4cadbd67: Pull complete
df11fe59eb47: Pull complete
ec04b821a79c: Pull complete
dd880bb86bec: Pull complete
40247f329eb4: Pull complete
3305f8696bbf: Pull complete
44b66140b403: Pull complete
72ad176c3ec5: Pull complete
Digest: sha256:8cea6fe3bb1304f889a8343944ce8ae3b93d42757888e84f3816d54d2765dac8
Status: Downloaded newer image for labtainers/capabilities.capabilities.student:latest
non-network local connections being added to access control list

Please enter your e-mail address: B20DAT098
Started 1 containers, 0 completed initialization, please wait...
```

Nhiệm vụ 1: Trải nghiệm Capabilities

Với tư cách là người dùng ubuntu không có đặc quyền

```
student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Help
latest: Pulling
ff94050018be: i
b49a4cadbd67: i
df11fe59eb47: i
ec04b821a79c: i
dd880bb86bec: i
40247f329eb4: i
3305f8696bbf: i
44b66140b403: i
72ad176c3ec5: i
Digest: sha256 64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=6 ttl=127 time=22.3 ms
non-network lo:64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=7 ttl=127 time=20.8 ms
Please enter y
Started 1 cont:64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=8 ttl=127 time=24.0 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=9 ttl=127 time=21.1 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=10 ttl=127 time=20.9 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=11 ttl=127 time=20.9 ms
The lab manual 64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=12 ttl=127 time=21.0 ms
file:///home^C
A lab report ti--- www.google.com ping statistics ---
file:///home12 packets transmitted, 12 received, 0% packet loss, time 11018ms
rtt min/avg/max/mdev = 20.830/21.767/25.002/1.313 ms
You may open tiubuntu@capabilities:~$
and select "Op:

Press <enter> to start the lab

student@ubuntu:~/labtainer/labtainer-student$
```

Bằng cách sử dụng capabilities, chúng ta có thể loại bỏ các đặc quyền không cần thiết từ ping.

```
student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Help

ubuntu@capabilities: ~
File Edit View Search Terminal Help
ubuntu@capabilities:~$ % ping www.google.com
-su: fg: %: no such job
ubuntu@capabilities:~$ ping www.google.com
PING www.google.com (172.217.31.4) 56(84) bytes of data.
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=1 ttl=127 time=21.1 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=2 ttl=127 time=25.0 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=3 ttl=127 time=21.7 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=4 ttl=127 time=20.9 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=5 ttl=127 time=21.1 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=6 ttl=127 time=22.3 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=7 ttl=127 time=20.8 ms

64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=8 ttl=127 time=24.0 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=9 ttl=127 time=21.1 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=10 ttl=127 time=20.9 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=11 ttl=127 time=20.9 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=12 ttl=127 time=21.0 ms
^C
--- www.google.com ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11018ms
rtt min/avg/max/mdev = 20.830/21.767/25.002/1.313 ms
ubuntu@capabilities:~$ sudo chmod u-s /bin/ping
ubuntu@capabilities:~$

Press <enter> to start the lab

student@ubuntu:~/labtainer/labtainer-student$
```

Chạy lại với lệnh “ping www.google.com” sau khi thực hiện lệnh sudo chmod u-s /bin/ping

```
student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Help

ubuntu@capabilities: ~
File Edit View Search Terminal Help
ubuntu@capabilities:~$ % ping www.google.com
-su: fg: %: no such job
ubuntu@capabilities:~$ ping www.google.com
PING www.google.com (172.217.31.4) 56(84) bytes of data.
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=1 ttl=127 time=21.1 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=2 ttl=127 time=25.0 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=3 ttl=127 time=21.7 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=4 ttl=127 time=20.9 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=5 ttl=127 time=21.1 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=6 ttl=127 time=22.3 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=7 ttl=127 time=20.8 ms

64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=8 ttl=127 time=24.0 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=9 ttl=127 time=21.1 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=10 ttl=127 time=20.9 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=11 ttl=127 time=20.9 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=12 ttl=127 time=21.0 ms
^C
--- www.google.com ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11018ms
rtt min/avg/max/mdev = 20.830/21.767/25.002/1.313 ms
ubuntu@capabilities:~$ sudo chmod u-s /bin/ping
ubuntu@capabilities:~$ ping www.google.com
ping: icmp open socket: Operation not permitted
ubuntu@capabilities:~$

Press <enter> to start the lab

student@ubuntu:~/labtainer/labtainer-student$
```

Ta gán capability cap_net_raw cho ping:
sudo setcap cap_net_raw=ep /bin/ping
sau đó chạy lệnh: ping www.google.com

```
student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Help

ubuntu@capabilities: ~
File Edit View Search Terminal Help
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=9 ttl=127 time=21.1 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=10 ttl=127 time=20.9 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=11 ttl=127 time=20.9 ms
64 bytes from hkg12s38-in-f4.1e100.net (172.217.31.4): icmp_seq=12 ttl=127 time=21.0 ms
^C
--- www.google.com ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11018ms
rtt min/avg/max/mdev = 20.830/21.767/25.002/1.313 ms
ubuntu@capabilities:~$ sudo chmod u-s /bin/ping
ubuntu@capabilities:~$ ping www.google.com
ping: icmp open socket: Operation not permitted
ubuntu@capabilities:~$ sudo setcap cap_net_raw=ep /bin/ping
ubuntu@capabilities:~$ ping www.google.com
PING www.google.com (142.250.204.132) 56(84) bytes of data:
64 bytes from hkg07s41-in-f4.1e100.net (142.250.204.132): icmp_seq=1 ttl=127 time=22.0 ms
64 bytes from hkg07s41-in-f4.1e100.net (142.250.204.132): icmp_seq=2 ttl=127 time=20.3 ms
64 bytes from hkg07s41-in-f4.1e100.net (142.250.204.132): icmp_seq=3 ttl=127 time=21.2 ms
64 bytes from hkg07s41-in-f4.1e100.net (142.250.204.132): icmp_seq=4 ttl=127 time=25.1 ms
64 bytes from hkg07s41-in-f4.1e100.net (142.250.204.132): icmp_seq=5 ttl=127 time=21.2 ms
64 bytes from hkg07s41-in-f4.1e100.net (142.250.204.132): icmp_seq=6 ttl=127 time=20.4 ms
^C
--- www.google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 20.397/21.750/25.107/1.598 ms
ubuntu@capabilities:~$
Press <enter> to start the lab

student@ubuntu:~/labtainer/labtainer-student$
```

Nhiệm vụ 1.1: Cho phép người dùng không đặc quyền chạy tcpdump

Chạy lệnh sudo tcpdump

```
ubuntu@capabilities:~$ which tcpdump
/usr/bin/tcpdump
ubuntu@capabilities:~$ sudo setcap cap_net_raw,cap_net_admin=ep /usr/bin/tcpdump
ubuntu@capabilities:~$ tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
ubuntu@capabilities:~$
```

Sửa đổi chương trình tcpdump để cho phép người dùng không đặc quyền chạy nó.

Nhiệm vụ 1.2: Chuyển đổi passwd để sử dụng capabilities

Sửa đổi chương trình passwd để sử dụng khả năng thay vì setuid, sau đó chứng minh rằng nó vẫn hoạt động bằng cách thay đổi mật khẩu của người dùng ubuntu

```
student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Help

ubuntu@capabilities: ~
File Edit View Search Terminal Help
PING www.google.com (216.58.203.68) 56(84) bytes of data.
64 bytes from kul09s03-in-f4.1e100.net (216.58.203.68): icmp_seq=1 ttl=127 time=20.5 ms
64 bytes from kul09s03-in-f4.1e100.net (216.58.203.68): icmp_seq=2 ttl=127 time=19.4 ms
64 bytes from kul09s03-in-f4.1e100.net (216.58.203.68): icmp_seq=3 ttl=127 time=23.7 ms
64 bytes from kul09s03-in-f4.1e100.net (216.58.203.68): icmp_seq=4 ttl=127 time=19.1 ms
^C
--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 19.180/20.733/23.773/1.835 ms
ubuntu@capabilities:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
ubuntu@capabilities:~$ sudo setcap cap_chown,cap_dac_override,cap_fowner+ep /usr/bin/tcpdump
ubuntu@capabilities:~$ sudo setcap cap_chown,cap_dac_override,cap_fowner+ep /usr/bin/passwd
ubuntu@capabilities:~$ passwd ubuntu
Changing password for ubuntu.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
ubuntu@capabilities:~$ █
Press <enter> to start the lab

student@ubuntu:~/labtainer/labtainer-student$ █
```

Nhiệm vụ 2: Điều chỉnh đặc quyền

```
ubuntu@capabilities: ~
File Edit View Search Terminal Help

^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
ubuntu@capabilities:~$ cat mypriv.c
/* mypriv.c
Simple example of dropping privileges within a
program that has been granted the
CAP_DAC_READ_SEARCH capability.
*/
#include <fcntl.h>
#include <sys/types.h>
#include <errno.h>
#include <stdlib.h>
#include <stdio.h>
#include <linux/capability.h>
#include <sys/capability.h>
int cap_disable(cap_value_t capflag);
int cap_enable(cap_value_t capflag);
int cap_drop(cap_value_t capflag);
int is_cap_set(cap_value_t capflag);
int main(void)
{
    if (is_cap_set(CAP_DAC_READ_SEARCH) == 0) {
        printf("CAP_DAC_READ_SEARCH capability is not set for this program\n");
        return -1;
    }
    if (open("/etc/shadow", O_RDONLY) < 0)
        printf("(a) Open failed\n");
    /* Question (a): is the above open successful? why? */
    if (cap_disable(CAP_DAC_READ_SEARCH) < 0) return -1;
    if (open("/etc/shadow", O_RDONLY) < 0)
        printf("(b) Open failed\n");
    /* Question (b): is the above open successful? why? */
    if (cap_enable(CAP_DAC_READ_SEARCH) < 0) return -1;
    if (open("/etc/shadow", O_RDONLY) < 0)
        printf("(c) Open failed\n");
    /* Question (c): is the above open successful? why? */
    if (cap_drop(CAP_DAC_READ_SEARCH) < 0) return -1;
```



```
ubuntu@capabilities: ~  
File Edit View Search Terminal Help  
/* Question (e): is the above open sucessful? why?*/  
}  
int is_cap_set(cap_value_t capflag)  
{  
    cap_t mycaps;  
    mycaps = cap_get_proc();  
    cap_flag_value_t cap_flags_value;  
    cap_get_flag(mycaps, capflag, CAP_EFFECTIVE, &cap_flags_value);  
    if(cap_flags_value == CAP_SET)  
        return 1;  
    else  
        return 0;  
}  
int cap_disable(cap_value_t capflag)  
{  
    cap_t mycaps;  
    mycaps = cap_get_proc();  
    if (mycaps == NULL)  
        return -1;  
    if (cap_set_flag(mycaps, CAP_EFFECTIVE, 1, &capflag, CAP_CLEAR) != 0)  
        return -1;  
    if (cap_set_proc(mycaps) != 0)  
        return -1;  
    return 0;  
}  
int cap_enable(cap_value_t capflag)  
{  
    cap_t mycaps;  
    mycaps = cap_get_proc();  
    if (mycaps == NULL)  
        return -1;  
    if (cap_set_flag(mycaps, CAP_EFFECTIVE, 1, &capflag, CAP_SET) != 0)  
        return -1;  
    if (cap_set_proc(mycaps) != 0)  
        return -1;  
    return 0;  
}  
int cap_drop(cap_value_t capflag)  
{  
}  
int cap_drop(cap_value_t capflag)  
{  
    cap_t mycaps;  
    mycaps = cap_get_proc();  
    if (mycaps == NULL)  
        return -1;  
    if (cap_set_flag(mycaps, CAP_EFFECTIVE, 1, &capflag, CAP_CLEAR) != 0)  
        return -1;  
    if (cap_set_flag(mycaps, CAP_PERMITTED, 1, &capflag, CAP_CLEAR) != 0)  
        return -1;  
    if (cap_set_proc(mycaps) != 0)  
        return -1;  
    return 0;  
}  
ubuntu@capabilities:~$
```

Câu hỏi (a): Câu lệnh open ("/etc/shadow", O_RDONLY) trả về giá trị -1, điều này có nghĩa rằng việc mở tệp /etc/shadow không thành công.

Câu hỏi (b): Câu lệnh open ("/etc/shadow", O_RDONLY) cũng trả về giá trị -1. Khi chúng ta gọi cap_disable(CAP_DAC_READ_SEARCH), chúng ta đã tắt khả năng CAP_DAC_READ_SEARCH, dẫn đến việc không thể đọc tệp /etc/shadow nữa.

Câu hỏi (c): Câu lệnh open ("/etc/shadow", O_RDONLY) trở thành thành công, không trả về giá trị -1. Sau khi chúng ta gọi cap_enable(CAP_DAC_READ_SEARCH), chúng ta đã bật lại khả năng CAP_DAC_READ_SEARCH, cho phép đọc tệp /etc/shadow.

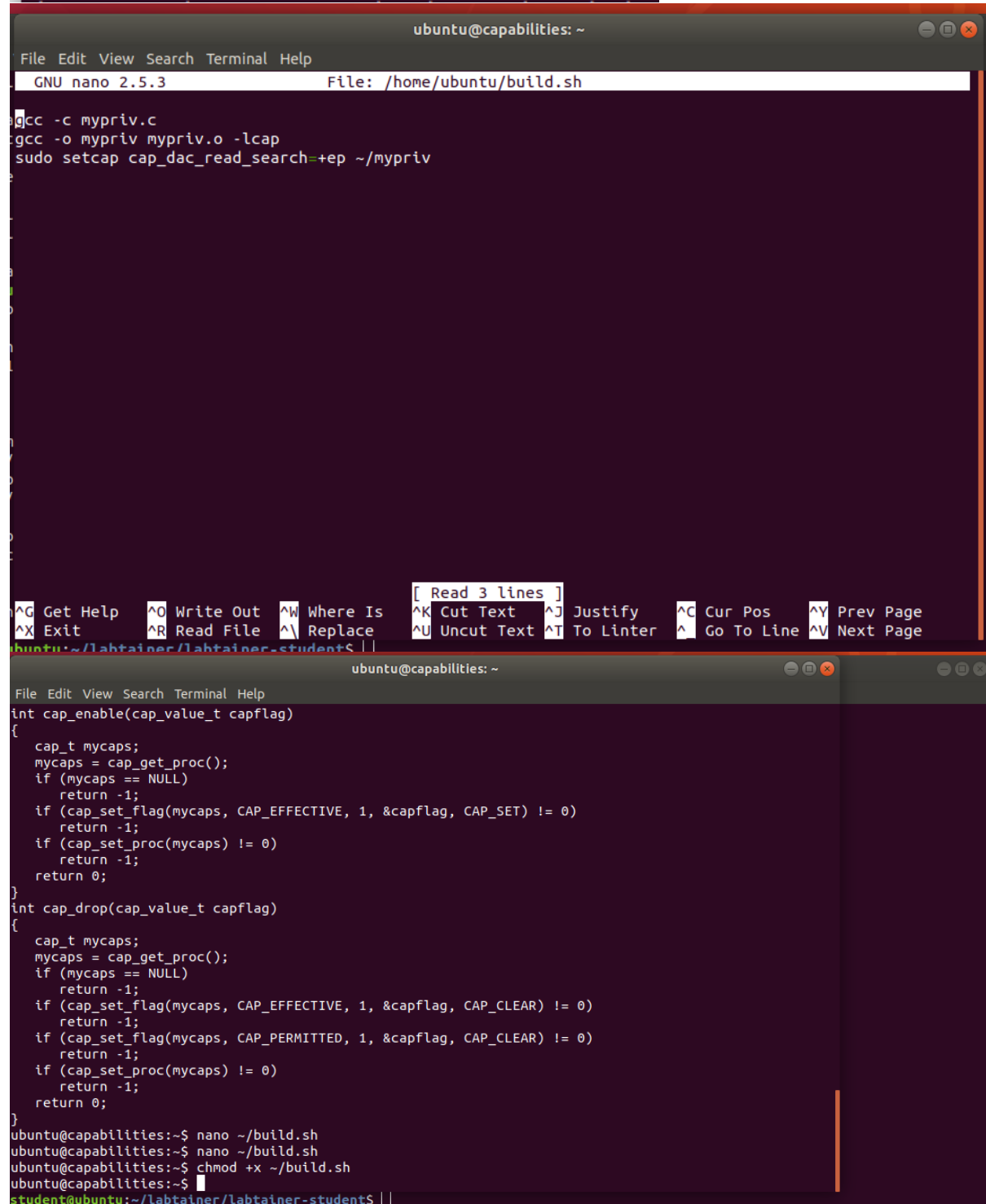
Câu hỏi (d): Câu lệnh open ("/etc/shadow", O_RDONLY) trả về giá trị -1. Sau khi chúng ta gọi cap_drop(CAP_DAC_READ_SEARCH), chúng ta đã loại bỏ khả năng CAP_DAC_READ_SEARCH, điều này dẫn đến việc không thể đọc tệp /etc/shadow nữa.

Câu hỏi (e): Câu lệnh open ("/etc/shadow", O_RDONLY) trở thành thành công, không trả về giá trị -1. Điều này xảy ra sau khi chúng ta gọi cap_enable(CAP_DAC_READ_SEARCH) để bật lại khả năng CAP_DAC_READ_SEARCH, cho phép đọc tệp /etc/shadow. Mã nguồn mypriv.c này giúp minh họa cách rơi bỏ quyền đặc biệt trong một chương trình đã được cấp quyền

CAP_DAC_READ_SEARCH. Chương trình sử dụng các hàm `cap_disable()`, `cap_enable()`, và `cap_drop()` để điều chỉnh trạng thái của khả năng CAP_DAC_READ_SEARCH. Việc rơi bỏ các quyền đặc biệt như vậy có thể giúp giảm tiềm năng rủi ro bảo mật trong các ứng dụng hệ thống.

- Vào file `build.sh`, thêm câu lệnh: `sudo setcap cap_dac_read_search=+ep ~/mypriv`

```
ubuntu@capabilities:~$ nano ~/build.sh
ubuntu@capabilities:~$ nano ~/build.sh
```



```
File Edit View Search Terminal Help
GNU nano 2.5.3 File: /home/ubuntu/build.sh

gcc -c mypriv.c
gcc -o mypriv mypriv.o -lcap
sudo setcap cap_dac_read_search=+ep ~/mypriv

[ Read 3 lines ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos ^V Prev Page
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Linter ^_ Go To Line ^V Next Page
ubuntu:~/labtainer/labtainer-student$
```

```
File Edit View Search Terminal Help
int cap_enable(cap_value_t capflag)
{
    cap_t mycaps;
    mycaps = cap_get_proc();
    if (mycaps == NULL)
        return -1;
    if (cap_set_flag(mycaps, CAP_EFFECTIVE, 1, &capflag, CAP_SET) != 0)
        return -1;
    if (cap_set_proc(mycaps) != 0)
        return -1;
    return 0;
}

int cap_drop(cap_value_t capflag)
{
    cap_t mycaps;
    mycaps = cap_get_proc();
    if (mycaps == NULL)
        return -1;
    if (cap_set_flag(mycaps, CAP_EFFECTIVE, 1, &capflag, CAP_CLEAR) != 0)
        return -1;
    if (cap_set_flag(mycaps, CAP_PERMITTED, 1, &capflag, CAP_CLEAR) != 0)
        return -1;
    if (cap_set_proc(mycaps) != 0)
        return -1;
    return 0;
}

ubuntu@capabilities:~$ nano ~/build.sh
ubuntu@capabilities:~$ nano ~/build.sh
ubuntu@capabilities:~$ chmod +x ~/build.sh
ubuntu@capabilities:~$
```

3. Checkwork

```
student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Help

student@ubuntu:~/labtainer/labtainer-student$ sudo tcpdump
[sudo] password for student:
student@ubuntu:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/capabilities
Trouble with zip file B20DCAT098.lab
[2023-09-25 03:18:32,343 - WARNING : gradelab:113 - CopyStudentArti() ] This file does not appear to be a result from lab
capabilities: /home/student/labtainer_xfer/capabilities/B20DCAT098.lab
Labname capabilities

Student | ping_use_cap | passwd_changed |
===== | ===== | ===== |
B20DCAT098 | Y | Y |
What is automatically assessed for this lab:

A subset of the lab goals.
ping_use_cap: Was setuid disabled on ping, and the net_raw capability set?
passwd_changed: Able to change password without suid on passwd?
student@ubuntu:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/capabilities
Labname capabilities

Student | ping_use_cap | passwd_changed |
===== | ===== | ===== |
B20DCAT098 | Y | Y |
What is automatically assessed for this lab:

A subset of the lab goals.
ping_use_cap: Was setuid disabled on ping, and the net_raw capability set?
passwd_changed: Able to change password without suid on passwd?
student@ubuntu:~/labtainer/labtainer-student$
```

4. Trả lời câu hỏi

Câu 1:

Trong tình huống mô tả của bạn, sau khi một chương trình vô hiệu hóa khả năng A, nó bị tấn công bởi một cuộc tấn công tràn bộ đệm và kẻ tấn công chèn mã độc vào không gian ngăn xếp của chương trình:

-Kẻ tấn công không thể sử dụng khả năng A nếu chương trình đã vô hiệu hóa nó: Nếu chương trình đã được vô hiệu hóa khả năng A, điều này có nghĩa là khả năng A không còn khả dụng cho chương trình đó. Dù kẻ tấn công có chèn mã độc vào không gian ngăn xếp, nó không thể sử dụng khả năng A trong quá trình thực thi mã độc đó.

-Kẻ tấn công không thể sử dụng khả năng A nếu quy trình xóa khả năng: Nếu quy trình xóa khả năng A đã được thực hiện, điều đó có nghĩa là khả năng A đã bị gỡ bỏ hoàn toàn khỏi chương trình. Ngay cả khi kẻ tấn công chèn mã độc vào không gian ngăn xếp, nó cũng không thể sử dụng khả năng A, vì nó đã bị xóa và không có sẵn trong chương trình nữa.

Câu 2:

Trong trường hợp cuộc tấn công được thay thế bằng cuộc tấn công đua điều kiện:

-Kẻ tấn công có thể sử dụng khả năng A nếu khả năng này bị tạm ngừng: Nếu khả năng A trong chương trình đã bị tạm ngừng, điều này có nghĩa là chương trình không thể sử dụng khả năng A trong quá trình thực thi bình thường. Tuy nhiên, nếu kẻ tấn công khai thác cuộc đua điều kiện và chèn mã độc vào chương trình, nó có thể tận dụng các điều kiện đặc biệt để kích hoạt lại khả năng A trong quá trình thực thi mã độc. Điều này có thể cho phép kẻ tấn công sử dụng khả năng A mà không cần phải dựa vào quá trình thực thi bình thường của chương trình.

-Kẻ tấn công không thể sử dụng khả năng nếu khả năng đã bị xóa: Nếu khả năng A đã bị xóa hoàn toàn khỏi chương trình, thì dù kẻ tấn công có khai thác cuộc đua điều kiện hoặc chèn mã độc vào chương trình, nó không thể sử dụng khả năng A. Việc xóa khả năng A đồng nghĩa với việc loại bỏ khả năng đó khỏi chương trình và không cho phép bất kỳ thực thể nào sử dụng nó, bao gồm cả kẻ tấn công.