

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



Môn học: An toàn ứng dụng Web và CSDL
Báo Cáo Thực Hành Lần 2

Họ và tên: Trần Thị Thu Phương

Mã sinh viên: B21DCAT151

Nhóm môn học: 03

Giảng viên: Vũ Minh Mạnh

Hà Nội, 2024

Mục lục

- 1. Kiểm soát chia sẻ thông tin trong CSDL SQL theo chính sách bảo mật 1**
- 2. Xác thực người dùng máy chủ Linux bằng dịch vụ LDAP4**

Bài thực hành 2

1. Kiểm soát chia sẻ thông tin trong CSDL SQL theo chính sách bảo mật

Nhiệm vụ 1: Bài kiểm tra trước khi bắt đầu lab

Bài tập Lịch sử Hỗ trợ

Trần Thị Thu Phương (B21DCAT151) 2:55:39

```
student@LabtainerVMware: ~/labtainer/labtainer-student
Question: It would be a policy violation if Alexander Hunold cannot
view his department (IT) salary range (T/F)?F
Correct. The policy allows Alexander to see his department's salary range, but
it does not require it.

Question: It would be a policy violation if David can view Susan's
salary (T/F)?T
Correct.

Question: It would be a policy violation if the database did not allow
Susan to modify family contact information for employees. (T/F)?T
Correct. The availability policy requires that HR be able to update employee
data in the database.

Question: It would be a policy violation if Susan can split the
employee table into two tables. (T/F)?T
Correct. Only the DBA is authorised to change the database schema

You answered all questions correctly.
student@LabtainerVMware:~/labtainer/labtainer-student$ S
```

Các câu hỏi trắc nghiệm

Nhiệm vụ 2: Khám phá

Trần Thị Thu Phương (B21DCAT151) 2:46:02

nancy@finance: ~

steven@executive: ~ x susan@hr: ~ x nancy@finance: ~ x david@it: ~ x

```
nancy@finance:~$ mysql -h database -u nancy -ppass4nancy
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 5.7.30-0ubuntu0.16.04.1-log (Ubuntu)
```

Từ máy finance bắt đầu 1 phiên MySQL với tên người dùng Nancy

Bài thực hành 2

Trên máy tính "database", bắt đầu một phiên MySQL với vai trò là admin để khám phá và đặt quyền truy cập cho người dùng



Bắt đầu một phiên MySQL với vai trò là admin

Nhiệm vụ 3: Kiểm soát quyền truy cập vào cơ sở dữ liệu

Là người quản trị cơ sở dữ liệu (DBA), bạn phải cấu hình cơ sở dữ liệu để áp dụng chính sách bảo mật thông tin đã được nêu trong phần Tổng quan, và cung cấp quyền truy cập dữ liệu cho người dùng như được nêu trong phần "Chỉ thị quản lý khác".

Sử dụng các lệnh SQL như REVOKE và GRANT để thay đổi quyền người dùng theo chính sách bảo mật. Đừng quên sử dụng lệnh FLUSH PRIVILEGES để áp dụng các thay đổi của bạn.

Hãy nhớ rằng tất cả người dùng đều yêu cầu truy cập để xem thông tin liên quan đến nhân viên bao gồm tên, email, số điện thoại, phòng ban, employee_id và manager_id.

LƯU Ý: Bên trong mỗi máy trạm, có một tệp <person>.sql. Những tệp tin này được sử dụng cho mục đích kiểm tra công việc. **KHÔNG CHỈNH SỬA** những tệp tin này.

Bài thực hành 2

Thực hành Bài tập Lịch sử Hỗ trợ

Trần Thị Thu Phương (B21DCAT151) 1:49:42

admin@database: ~

```
mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)

mysql> show grants for 'nancy'@'finance';
+-----+
| Grants for nancy@finance |
+-----+
| GRANT SELECT, CREATE, DROP, RELOAD, SHUTDOWN, PROCESS, FILE, REFERENCES, INDEX, ALTER, SHOW DATABASES, SUPER, CREATE TEMPORARY TABLES, LOCK TABLES, EXECUTE, REPLICATION SLAVE, REPLICATION CLIENT, CREATE VIEW, SHOW VIEW, CREATE ROUTINE, ALTER ROUTINE, CREATE USER, EVENT, TRIGGER, CREATE TABLESPACE ON *.* TO 'nancy'@'finance' |
+-----+
```

1

Kiểm tra quyền trong CSDL của 1 user từ một host

https://seclab.ptit.edu.vn/student/history

Trần Thị Thu Phương (B21DCAT151) 1:37:54

admin@database: ~

```
your MySQL server version for the right syntax to use near 'TO 'david'@'it'' at line 1
mysql> REVOKE ALL PRIVILEGES ON *.* FROM 'david'@'it';
Query OK, 0 rows affected (0.00 sec)

mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)

mysql> show grants for 'david'@'it';
+-----+
| Grants for david@it |
+-----+
| GRANT USAGE ON *.* TO 'david'@'it' |
+-----+
1 row in set (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON *.* TO 'david'@'it';
Query OK, 0 rows affected (0.00 sec)

mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)

mysql>
```

Cấp tất cả các quyền cho david@it

Trần Thị Thu Phương (B21DCAT151) 1:49:23

```
admin@database: ~  
-----+-----  
| GRANT SELECT, CREATE, DROP, RELOAD, SHUTDOWN, PROCESS, FILE, REFERENCES, INDEX, ALTER, SHOW  
DATABASES, SUPER, CREATE TEMPORARY TABLES, LOCK TABLES, EXECUTE, REPLICATION SLAVE, REPLICATIO  
N CLIENT, CREATE VIEW, SHOW VIEW, CREATE ROUTINE, ALTER ROUTINE, CREATE USER, EVENT, TRIGGER,  
CREATE TABLESPACE ON *.* TO 'nancy'@'finance' |  
-----+-----  
1 row in set (0.00 sec)  
  
mysql> REVOKE SELECT, SHOW DATABASES ON *.* FROM 'nancy'@'finance';  
  
Query OK, 0 rows affected (0.00 sec)  
  
mysql> flush privileges;  
Query OK, 0 rows affected (0.00 sec)  
  
mysql>
```

Thu hồi quyền SELECT, SHOW DATABASES của người dùng nancy@finance

2. Xác thực người dùng máy chủ Linux bằng dịch vụ LDAP

Nhiệm vụ 1: Tìm hiểu

Trên máy chủ LDAP, hiển thị nội dung thư mục LDAP bằng cách sử dụng lệnh:

ldapsearch -x | less

Và quan sát các mục trong thư mục. Lưu ý mục cho "mike" và "projx".

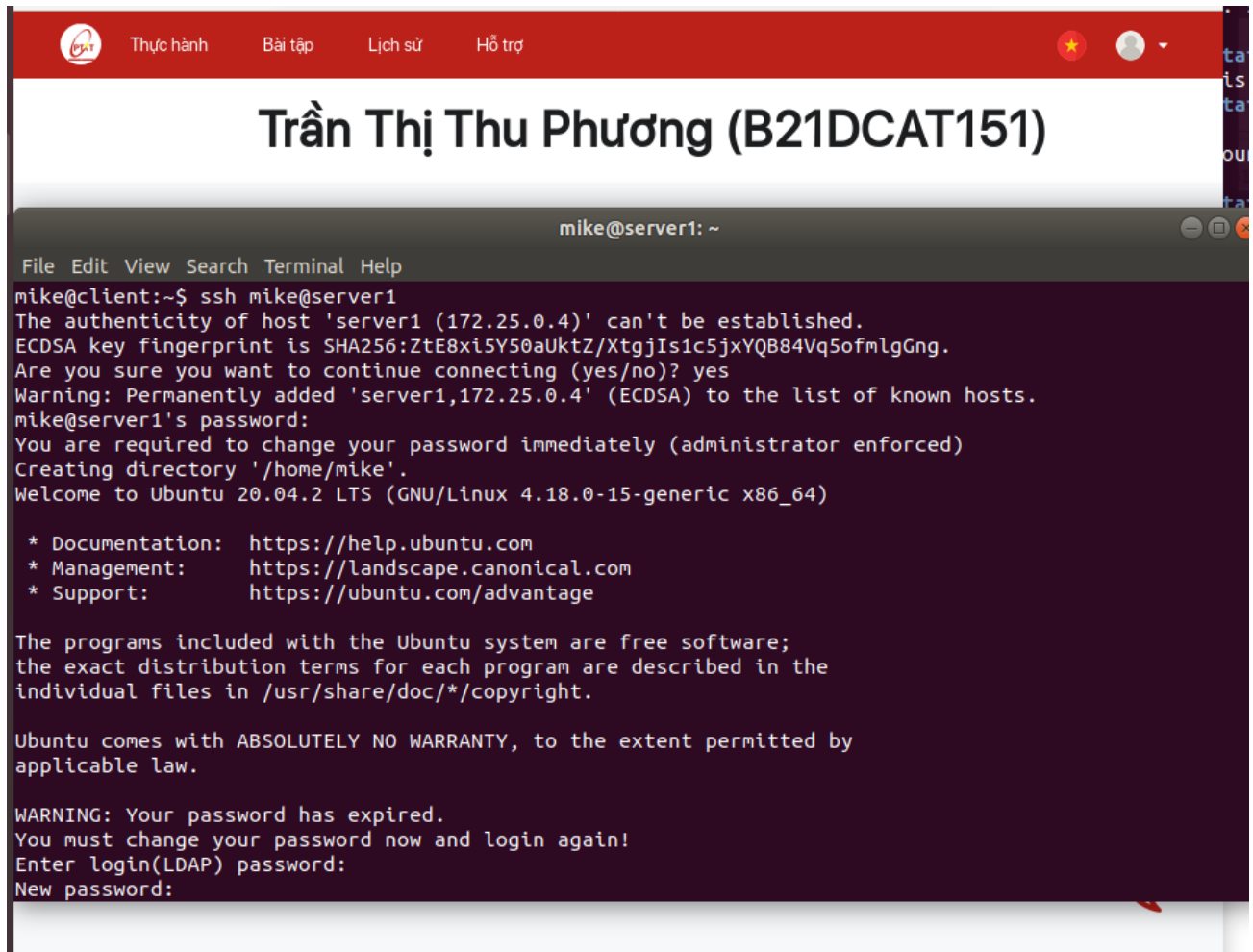
Bắt đầu Wireshark trên thành phần LDAP để có thể quan sát giao thức: wireshark &

```
← → ↺ ↻ 🔒 https://seclab.ptit.edu.vn/student/contest/ 90% ... ☆  
PTIT Thực hành Bài tập Lịch sử Hỗ trợ  
  
Trần Thị Thu Phương (B21DCAT151)  
  
admin@ldap: ~  
File Edit View Search Terminal Help  
admin@ldap:~$ ldapsearch -x | less  
admin@ldap:~$ wireshark &  
[1] 595  
admin@ldap:~$
```

Từ máy tính "client", kết nối SSH đến server1 với người dùng "mike":

```
ssh mike@server1
```

Mật khẩu ban đầu cho "mike" là "password123". Hệ thống sẽ yêu cầu thay đổi mật khẩu này, sau đó cần kết nối SSH lại vào server1. Thay đổi mật khẩu thành một mật khẩu bất kỳ. Sử dụng SSH một lần nữa để đăng nhập vào server1 với vai trò là *mike*, cung cấp mật khẩu mới.



```
Trần Thị Thu Phương (B21DCAT151)

mike@server1: ~
File Edit View Search Terminal Help
mike@client:~$ ssh mike@server1
The authenticity of host 'server1 (172.25.0.4)' can't be established.
ECDSA key fingerprint is SHA256:ZtE8xi5Y50aUktZ/XtgjIs1c5jxYQB84Vq5ofmlgGng.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server1,172.25.0.4' (ECDSA) to the list of known hosts.
mike@server1's password:
You are required to change your password immediately (administrator enforced)
Creating directory '/home/mike'.
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 4.18.0-15-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

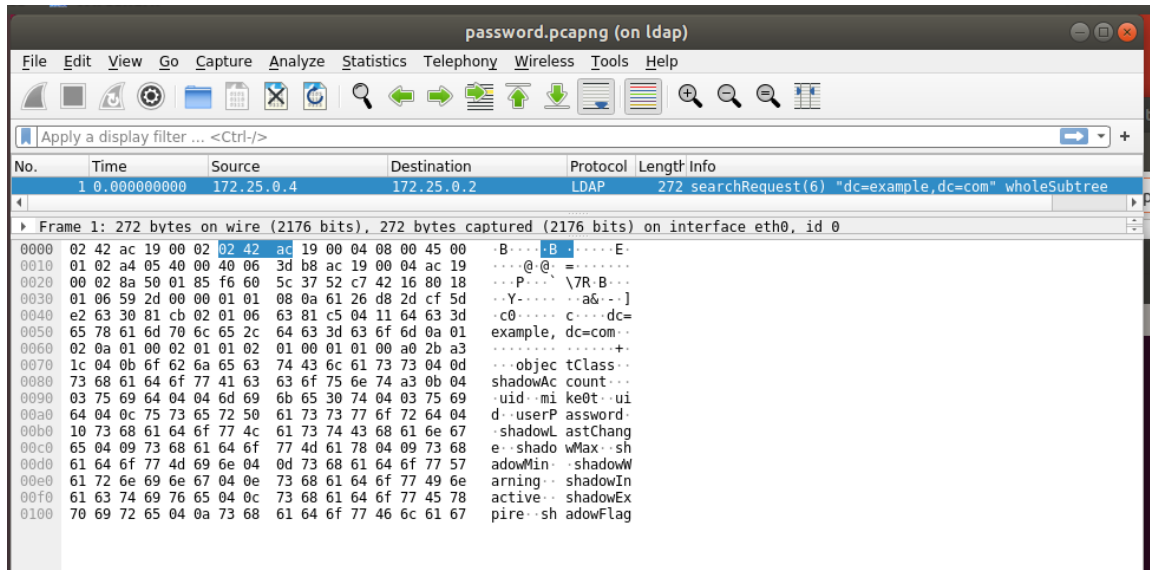
WARNING: Your password has expired.
You must change your password now and login again!
Enter login(LDAP) password:
New password:
```

Từ máy client kết nối SSH đến server1 với người dùng "mike"

Nhiệm vụ 2: Xem lưu lượng giao thức

Chuyển đến cửa sổ Wireshark và dừng việc bắt gói tin (ví dụ: nút dừng màu đỏ). Nhập bộ lọc hiển thị là "ldap" vào ô gần đầu "Áp dụng bộ lọc hiển thị...". Xem lại lưu lượng LDAP. Các thành phần nào đang trao đổi gói tin? Tìm gói tin đã thay đổi mật khẩu của mike và sử dụng File / Export Specified Packets để lưu gói tin đó vào tệp có tên password.pcapng.

Bài thực hành 2

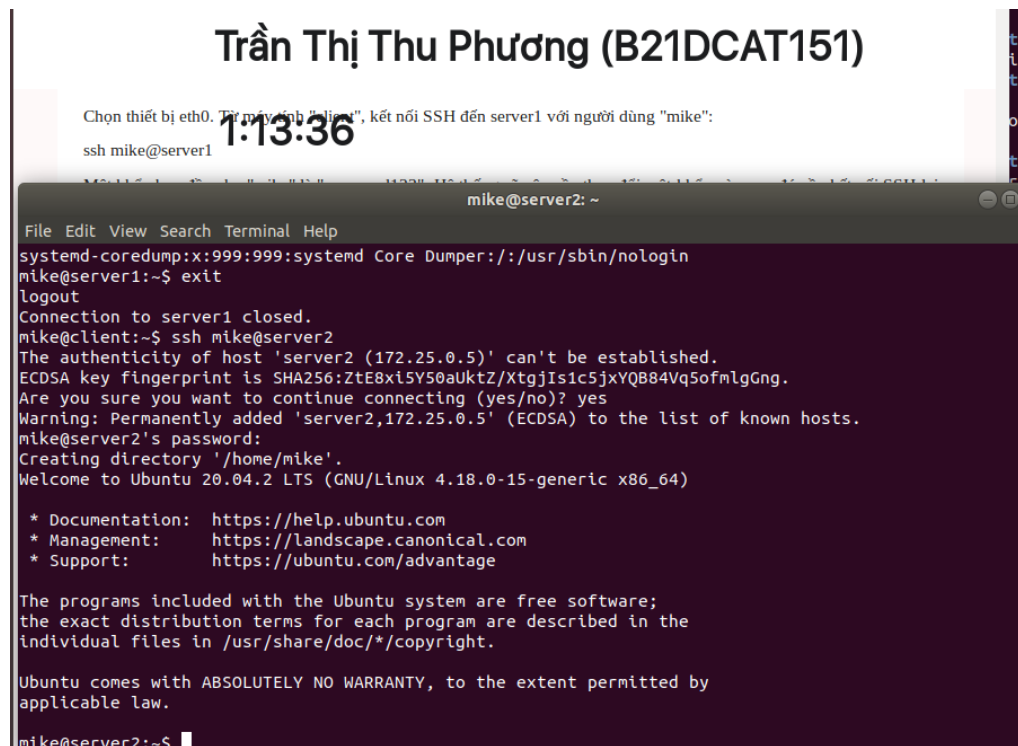


Tệp password.pcapng

Nhiệm vụ 3: Sử dụng tài khoản mike để truy cập máy chủ còn lại

Thoát khỏi phiên SSH đến server1 bằng cách nhập lệnh "exit". Sau đó, SSH đến server2 bằng cách nhập lệnh "ssh mike@server2". Mật khẩu bạn mong đợi sử dụng để xác thực đến server2 là mật khẩu mới mà bạn đã thay đổi trên server1.

Sau khi đăng nhập vào server2, thoát khỏi phiên SSH đó bằng cách nhập lệnh "exit".



Kết nối SSH

Nhiệm vụ 4: Thêm một người dùng LDAP

Tạo tệp qa.ldif sẽ được sử dụng cho người dùng Mary

A screenshot of a terminal window titled "Trần Thị Thu Phương (B21DCAT151) 02:42". The terminal shows the command "cat qa.ldif" and its output, which is an LDAP entry for Mary Smith. The entry includes fields for dn, objectClass, uid, cn, sn, userPassword, uidNumber, gidNumber, and homeDirectory.

```
admin@ldap: ~  
File Edit View Search Terminal Help  
admin@ldap:~$ cat qa.ldif  
dn: uid=mary,ou=users,dc=example,dc=com  
objectClass: inetOrgPerson  
objectClass: posixAccount  
objectClass: organizationalPerson  
uid: mary  
cn: Mary Smith  
sn: Smith  
userPassword: password123  
uidNumber: 1502  
gidNumber: 1002  
homeDirectory: /home/mary  
admin@ldap:~$
```

Nội dung của tệp qa.lif

Sau đó, chuyển đến máy khách và kiểm tra khả năng để SSH với vai trò là *mary* đến cả server1 và server2.

A screenshot of a terminal window titled "Trần Thị Thu Phương (B21DCAT151) 01:39". The terminal shows the user "mike@client" performing several actions: creating a directory, displaying Ubuntu welcome messages, exiting, and then connecting to server1 via SSH as the user "mary".

```
mike@client: ~  
File Edit View Search Terminal Help  
Creating directory '/home/mary'.  
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 4.18.0-15-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
$ exit  
Connection to server2 closed.  
mike@client:~$ ssh mary@server1  
mary@server1's password:  
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 4.18.0-15-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
Last login: Wed Oct  2 04:55:08 2024 from 172.25.0.3  
$
```

Bài thực hành 2

SSH từ máy client đến server1 dưới user mary vừa tạo

```
student@ubuntu:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/ldap
Labname ldap

Student          | correct_pcap | mike_server1 | mike_server2 | mary_server1 | mary_server2 |
=====|=====|=====|=====|=====|=====|
B21DCAT151       |              Y |              Y |              Y |              Y |              Y |
What is automatically assessed for this lab:
mike_server1, mike_server2, mary_server1, mary_server2, pcap_strings, _pcap_pass: user initiated session on the
server
```

Checkwork