**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

Môn: HỆ ĐIỀU HÀNH WINDOWS VÀ LINUX/UNIX

**BÁO CÁO BÀI THỰC HÀNH**

Tìm hiểu về dịch vụ xác thực LDAP

Họ và tên sinh viên: Lê Anh Tuấn

Mã số sinh viên: B21DCAT205

Họ và tên giảng viên: TS. Đinh Trường Duy

Hà Nội 11 năm 2023

**1. GIỚI THIỆU BÀI THỰC HÀNH**

**1.1 Mục đích**

- Bài thực hành này minh họa việc sử dụng LDAP để xác thực người dùng trên hệ thống Linux, sao cho nhiều máy tính chia sẻ một kho thông tin người dùng và nhóm duy nhất, bao gồm cả mật khẩu xác thực người dùng. Chiến lược này cho phép người dùng và quản trị viên quản lý một tập hợp thông tin đăng nhập duy nhất có thể được sử dụng để truy cập vào nhiều máy tính.

**1.2 Yêu cầu**

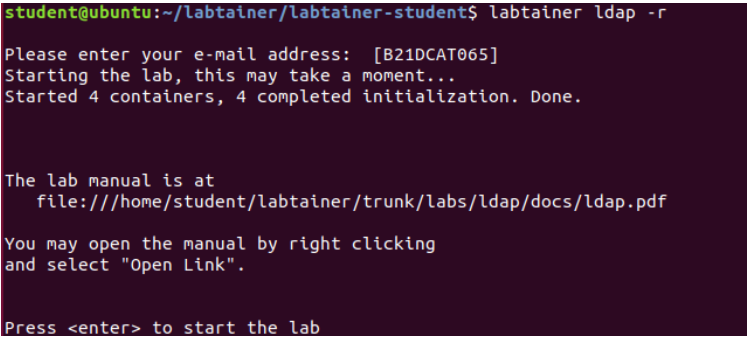
- Nắm được kiến thức về các kiến thức cơ bản của người dùng, nhóm và xác thực trong Linux, ví dụ như các tệp /etc/passwd và /etc/shadow. Ngoài ra, cần có kiến thức cơ bản về việc sử dụng Lightweight Directory Access Protocol (LDAP).

**2 NỘI DUNG THỰC HÀNH**

**Chuẩn bị lab**

Khởi động lab:

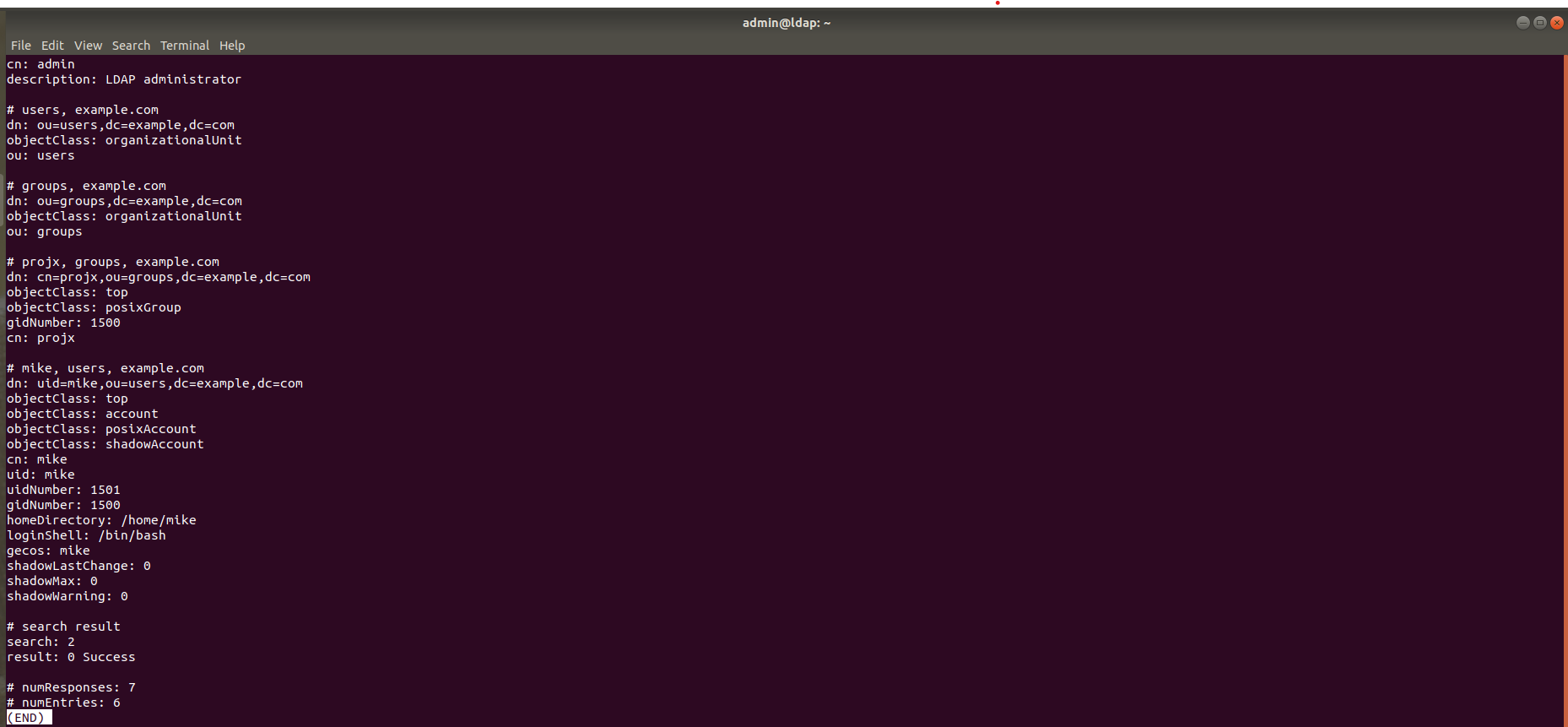
labtainer –r ldap



Chúng ta có 3 Terminal hiện ra, 1 là admin@ldap, 2 là mike@client, 3 là admin@server1 và admin@server2 cùng chung 1 terminal.

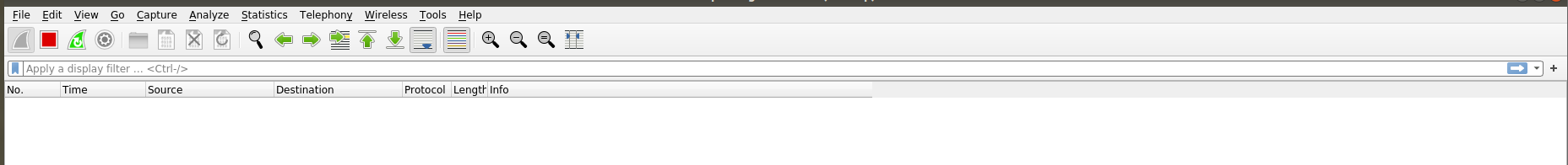
**Nhiệm vụ 1:** Tìm hiểu

Trước tiên ta sử dụng lệnh ldapsearch -x | less trên admin@ldap để xem thông tin thư mục ldap, bao gồm thông tin các user, các group trong miền example.com. Lưu ý mục “mike” và “projx” vì nhiệm vụ sau sẽ sử dụng đến

****

Khởi động **wireshark** trên **admin@ldap** và chọn bộ lọc thiết bị **eth0**:

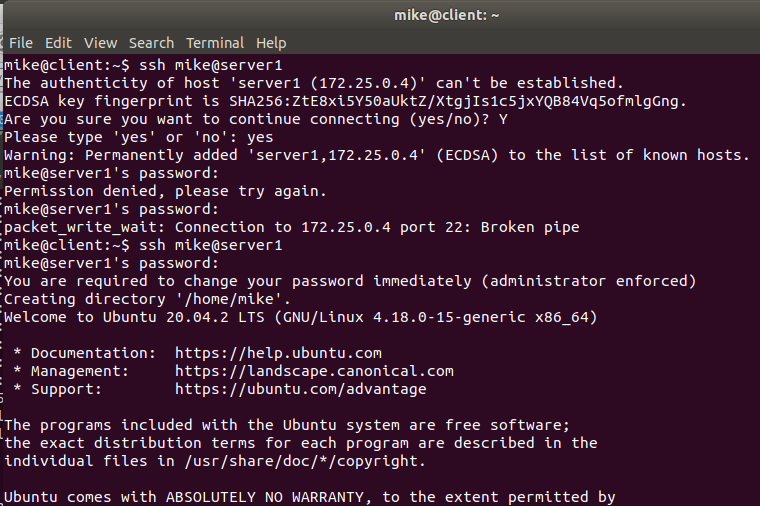
wireshark &

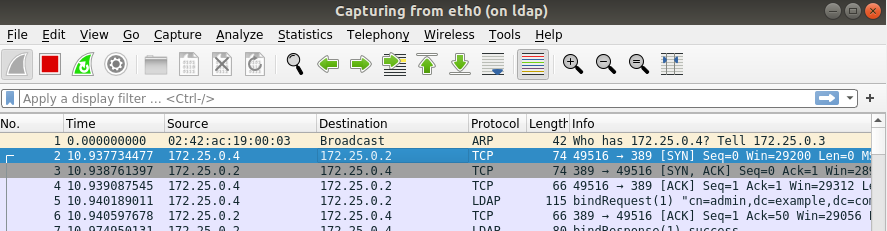


Chọn thiết bị **eth0**. Từ máy tính **client**, kết nối SSH đến **server1** với người dùng "mike" , mật khẩu là **password123**

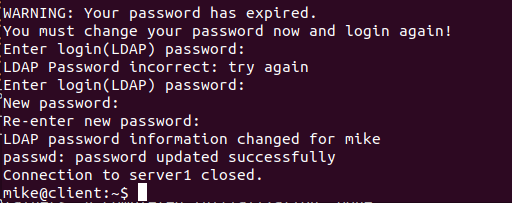
ssh mike@server1

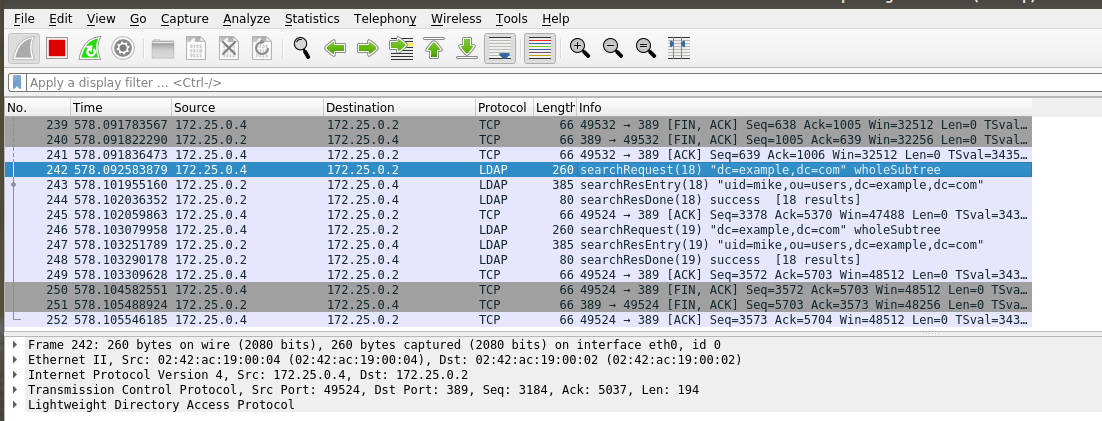
Vì sử dụng ssh để kết nối nên Server sẽ sử dụng key để mã hóa mật khẩu, từ đó chúng ta có thể thấy trên wireshark các gói tin chúng ta bắt được



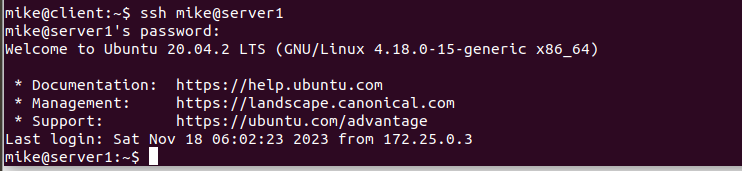
****

Hệ thống yêu cầu ta đổi mật khẩu do mật khẩu cũ đã hết hạn, ta đổi mật khẩu thành **tuan123**, các tiến trình vẫn được bắt trong phần **wireshark**

****

****

Đăng nhập lại với mật khẩu mới, ta đã vào được **server1** với tài khoản “mike”

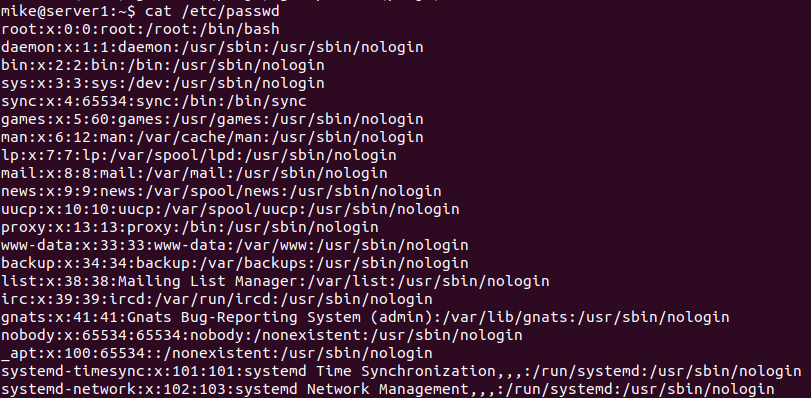
****

Dùng lệnh id để kiểm tra **userID** và **groupID** của “mike”

****

Từ đây biết được id của mike là 1501 và gourp của mike là projx với id là 1500 đúng như khi ta dùng lệnh **ldapsearch** tại **admin@ldap**.

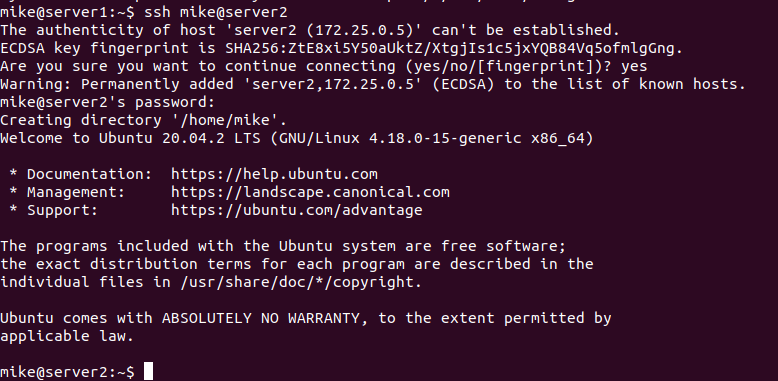
Ta dùng lệnh cat /etc/passwd để kiểm tra người dùng và nhóm

****

**Nhiệm vụ 2:**Xem lưu lượng giao thức

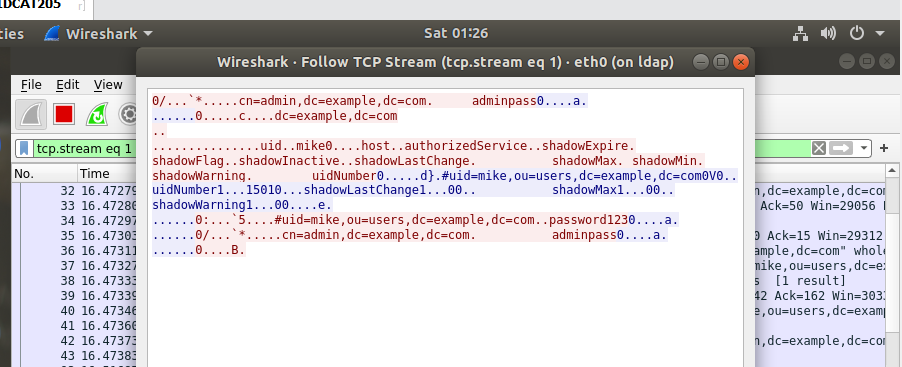
Ta thấy rằng hiện đang có root, admin là đang login.

Tiện đây chúng ta sẽ đăng nhập vào user “mike” ở server2 luôn với câu lệnh **ssh** **mike@server2** và mật khẩu là **tuan123**

****

Tiếp theo ta sẽ tìm gói tin đã thay đổi mật khẩu của “mike” .

Với giao thức truyền tin là ldap, ta sử dụng filter ldap để lọc các giao thức này ra. Follow và chọn tcp stream, ta nhận được các thông tin trông có phần giống với khi ta dùng lệnh **ldapsearch** ban đầu => wireshark đã bắt toàn bộ thông tin khi chúng ta đăng nhập vào máy chủ ldap



Về dữ liệu trong ldap thì thông tin trong ldap sẽ lưu trữ ở các file .ldif trong đó sẽ chứa thông tin về người dùng, mật khẩu (mã hóa) **userID** và **groupID** của người dùng cũng như group đó

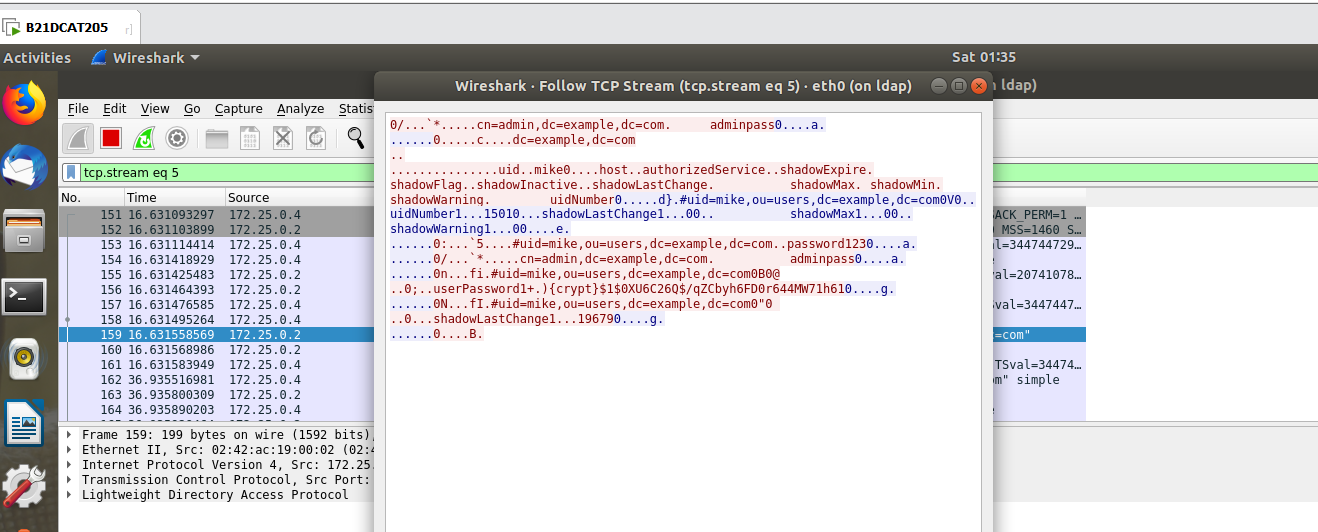
Và nếu như userPassword của 1 user nào đó được đổi thì định dạng đổi sẽ có dạng

**userPassword: {crypt}x**

Vậy nên trong wireshark ta sẽ tìm gói tin có định dạng trên => gói tin đó chính là

gói tin đổi mật khẩu người dùng “mike”

Chọn **File** => **Export Specified Packets** => **Selected Packets only** => lưu tên file là **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".

**Nhiệm vụ 4:**Thêm một người dùng LDAP

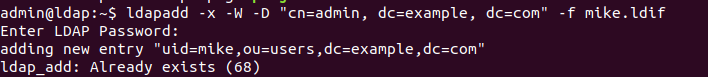
Chuyển đến cửa sổ terminal ảo LDAP và sử dụng lệnh ls để xem danh sách thư mục.

****

Xem tệp có tên mike.ldif, tệp này được sử dụng để định nghĩa người dùng có tên "mike". Sau đó, xem tệp projx.ldif. Lệnh LDAP được sử dụng để thêm mục đã định nghĩa trong tệp mike.ldif là:

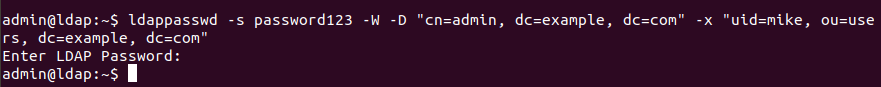
ldapadd -x-W -D "cn=admin,dc=example,dc=com" -f mike.ldif

Với -x là định nghĩa bình thường; -W là mật khẩu admin sẽ được ẩn; -D là chỉ định admin (mật khẩu admin là adminpass).

****

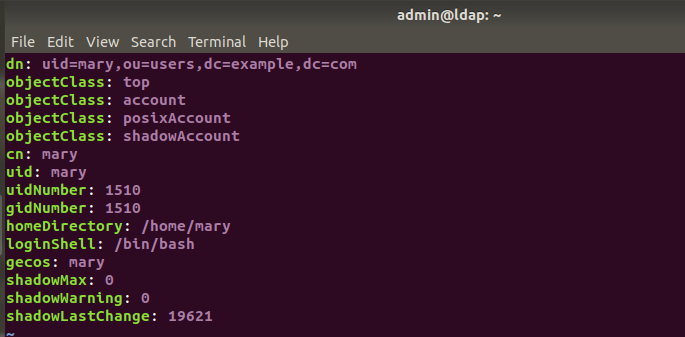
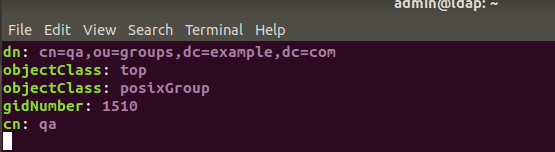
Sau đó có thể cấp cho người dùng mật khẩu mặc định (mật khẩu ban đầu) với câu lệnh:

ldappasswd-s password123-W-D"cn=admin,dc=example,dc=com" -x "uid=mike,ou=users,dc=example,dc=com"

****

Ta thử tạo một nhóm mới có tên “qa” và 1 người dùng mới có tên “mary”, gán mary vào nhóm qa. Trong admin ldap tạo 2 file .ldif mới có tên mary.ldif và qa.ldif bằng câu lệnh:

vi mary.ldif và vi qa.ldif

** **

Sau đó ấn **ESC** và **:wq** để lưu file và thoát khỏi phần soạn thảo Sử dụng các lệnh ldapadd cho 2 file .ldif trên và lệnh ldappasswd cho người dùng “mary”

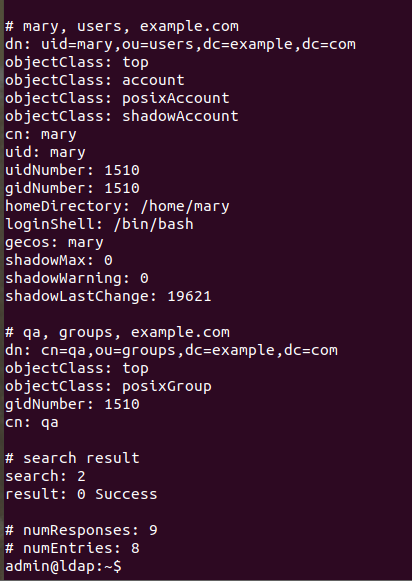
****

****

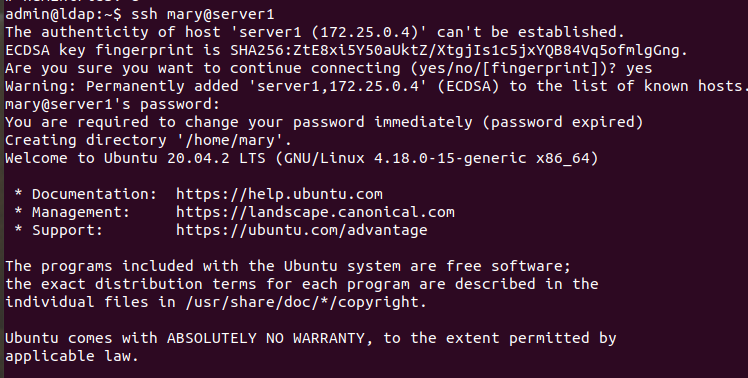
****

Đã hoàn thành tạo người dùng “mary” và nhóm “qa”.

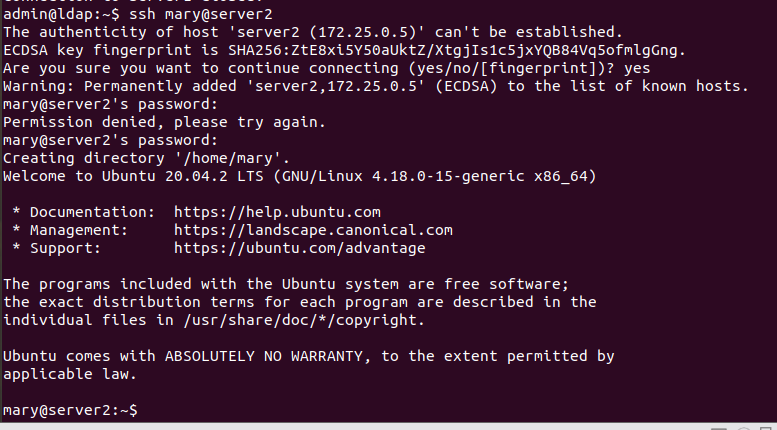
Dùng ldapsearch -x để kiểm tra xem người dùng và nhóm đã được thêm vào ldap chưa

****

Đã thêm thành công.

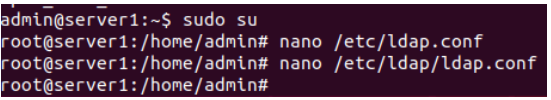
****

Thử đăng nhập vào server1 và server2 của ldap với người dùng “mary” mật khẩu “password123” thì server sẽ yêu cầu đổi lại mật khẩu, tôi đổi thành “tuan123”

****

**Nhiệm vụ 5:** Mã hóa dữ liệu truyền LDAP

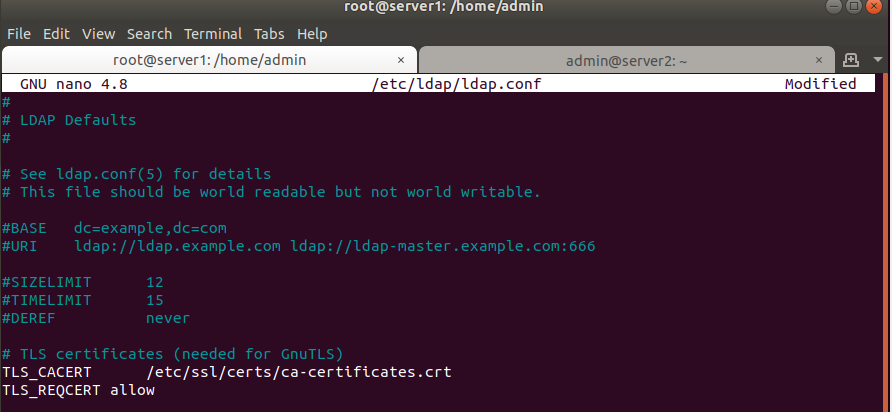
Ta sử dụng sudo su để vào chương trình root sau đó dùng lệnh nano để chỉnh sửa file **/etc/ldap.conf** và file **/etc/ldap/ldap.conf** của server1 và server2



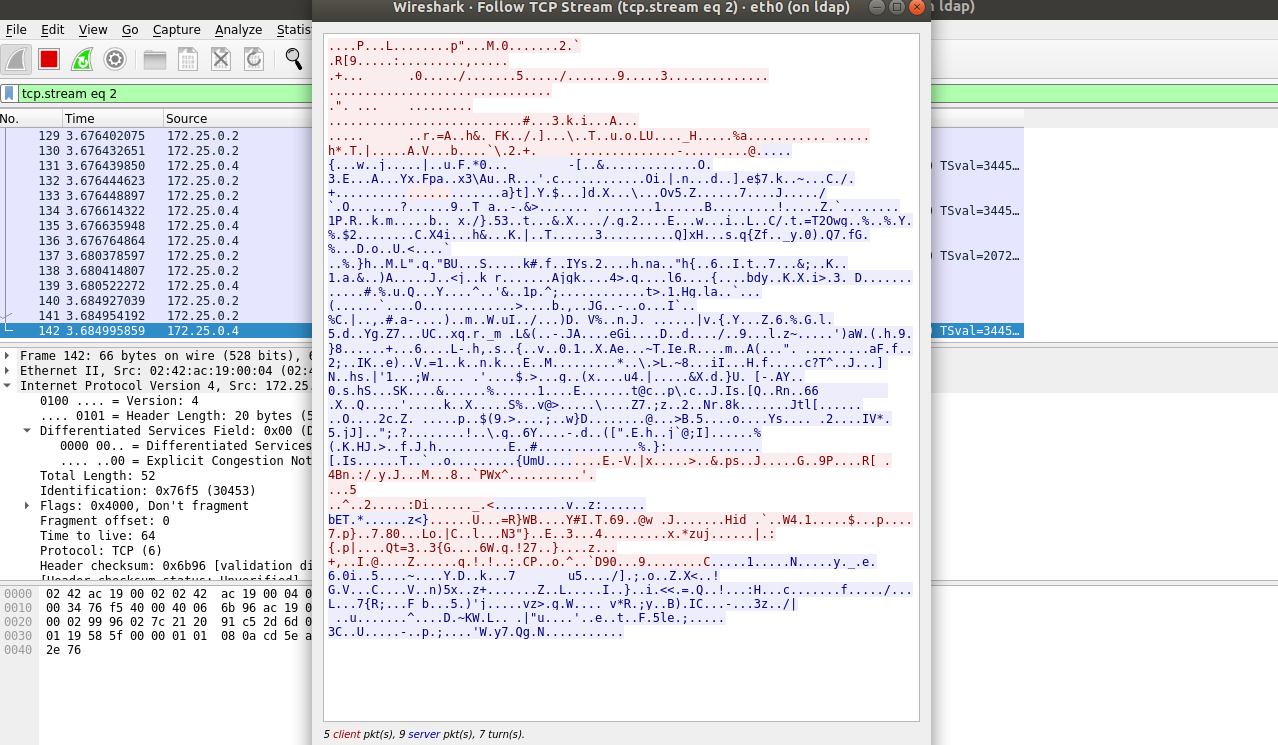
Chỉnh sửa tệp **/etc/ldap.conf** và thay đổi dòng sau: **uri ldap://ldap** **thành uri ldaps://ldap** và xóa dấu chú thích khỏi dòng: **#ssl on** sẽ trở thành: **ssl on**

** **

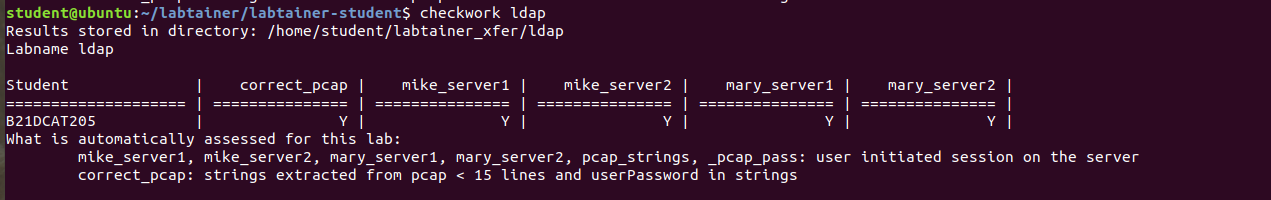
Sau đó, chỉnh sửa tệp **/etc/ldap/ldap.conf** (lưu ý thư mục khác biệt!) và thêm dòng này vào cuối tệp: **TLS\_REQCERT allow**



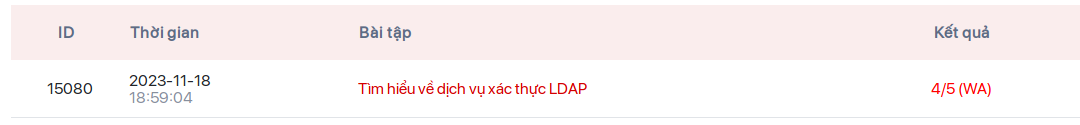
Thử connect lại bằng tài khoản mike ta thấy thông tin đã được mã hóa.

****

**Checkwork bài làm**

****

**Kết quả nộp bài**

****