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

BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: AN TOÀN MẠNG NÂNG CAO
MÃ HỌC PHẦN: INT1483

BÀI THỰC HÀNH
Openssl

Sinh viên thực hiện: Trần Thị Thu Phương

Mã sinh viên: B21DCAT151

Giảng viên hướng dẫn: TS. Phạm Hoàng Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

Khởi động bài lab**:**

Vào terminal gõ :

imodule https://github.com/lvkien19112001/imodule1/raw/main/imodule.tar

labtainer -r ptit-openssl

(chú ý: sinh viên sử dụng email stu.ptit.edu.vn của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

Sau khi khởi động xong hai terminal ảo sẽ xuất hiện, một cái là đại diện cho máy khách: client , một cái là đại diện cho máy chủ: server. Biết rằng 2 máy nằm cùng mạng LAN.

Task 1 : Kết nối Telnet từ client đến server.

- Trên terminal server sử dụng lệnh "ipconfig" để xác định địa chỉ IP
- Trên máy client thực thi lệnh

telnet <ip_server>

để kết nối máy client với máy server qua giao thức telnet.

(Lưu ý : Tài khoản , mật khẩu của máy server đều là " ubuntu ".)

```
File  Edit  View  Search  Terminal  Help
ubuntu@client:~$ telnet 172.20.0.20
Trying 172.20.0.20...
Connected to 172.20.0.20.
Escape character is '^]'.
Ubuntu 16.04.4 LTS
server login: ubuntu
Password:
Welcome to Ubuntu 16.04.4 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.
```

- Thực hiện đọc file .txt

```
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.

ubuntu@server:~$ ls
hash.enc  password.txt  personalize.txt
ubuntu@server:~$ cat password.txt
cat: password.txt: Permission denied
ubuntu@server:~$ sudo -s
root@server:~# cat password.txt
123
root@server:~# cat personalize.txt
My string is : fc09d54ecafd7206c31fa0a409bac0a2
root@server:~#
```

Task 2 : Lấy file thành công từ server về client.

- Tiến hành copy file từ server về client bằng dòng lệnh scp
- File lấy về có đuôi .enc. 172.20.0.20

```
Last login: Wed Mar 26 09:00:40 UTC 2025 from ptit-openssl.client.student.some_network on pts/2
Welcome to Ubuntu 16.04.4 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
ubuntu@server:~$ ls
hash.enc  password.txt  personalize.txt  ubuntu@172.20.0.10  ubuntu@client
ubuntu@server:~$ scp hash.enc ubuntu@172.20.0.10:~/
The authenticity of host '172.20.0.10 (172.20.0.10)' can't be established.
ECDSA key fingerprint is SHA256:tUpZwhy4nZSdmfsbuB5DUJ+CU5qwoSVPuLl59bbNnY0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.20.0.10' (ECDSA) to the list of known hosts.
ubuntu@172.20.0.10's password:
hash.enc                                      100%   40     0.0KB/s   00:00
ubuntu@server:~$
```

- Thoát khỏi máy server để trở về máy client và kiểm tra xem đã thấy file ở máy client hay chưa.

```
Connection closed by foreign host.
ubuntu@client:~$ ls
hash.enc
ubuntu@client:~$
```

Task 3 : Tiến hành giải mã file.

- Dùng câu lệnh

" openssl enc -des3 -in <file cần được giải mã> -d -out <file đã được giải mã> "

để tiến hành giải mã và yêu cầu một mật khẩu để giải mã .

- Công cuộc ở đây là cần tìm mật khẩu giải mã bên máy server để có thể tiến hành giải mã , và file mật khẩu giải mã nằm bên phía server.

  (Gợi ý : chạy quyền root để lấy mật khẩu)

- Tiến hành đọc file vừa được giải mã lấy được keyword.

Mật khẩu là: 123

```
My string is : Hashing
ubuntu@client:~$ openssl enc -des3 -in hash.enc -d -out hash.dec
enter des-ede3-cbc decryption password:
ubuntu@client:~$ ls
hash.dec  hash.enc  result.txt  text151.txt
ubuntu@client:~$ cat hash.dec
My string is : Hashing
ubuntu@client:~$
```

Kết thúc bài lab.

- Thực hiện checkwork:

checkwork ptit-openssl

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

Student              |          telnet |       copy_file |         hashing |
==================== | =============== | =============== | =============== |
B21DCAT151           |               Y |               Y |               Y |
What is automatically assessed for this lab:
        hashing: Failed login as expected.

student@ubuntu:~/labtainer/labtainer-student$ echo "Tran Thi Thu Phuong - B21DCAT151"
Tran Thi Thu Phuong - B21DCAT151
student@ubuntu:~/labtainer/labtainer-student$ date
Sun Apr 20 06:12:07 PDT 2025
student@ubuntu:~/labtainer/labtainer-student$
```

- Thực hiện đánh giá kết quả:

gradelab ptit-openssl

- Kết thúc bài lab:

stoplab ptit-openssl

- Khởi động lại bài lab:

labtainer -r ptit-openssl