SSH / SCP

Content

- Sử dụng cơ bản
- Cơ chế hoạt động
- SSH sử dụng key
- Thay đổi SSH port

SSH

SSH là gì?

SSH (Secure Shell): giao thức hỗ trợ truy cập vào máy chủ từ xa thông qua mạng Internet một cách an toàn.

SSH thiết lập một kết nối được bảo mật bằng mật mã giữa hai bên (client và server), xác thực mỗi bên với bên còn lại, đồng thời chuyển các lệnh và xuất qua lại.

Thường giao tiếp qua cổng 22

SSH

SSH xác thực người dùng

SSH Password	SSH Key
- Kiểm tra tên người dùng và mật khẩu, nếu đúng sẽ chấp thuận yêu cầu - Ưu điểm: Thuận tiện cho người dùng - Nhược điểm: Có thể bị tấn công vét cạn	- Một cặp SSH Key: Public Key và Private Key được tạo trên máy tính - Public Key được lưu trữ trên Server, Private Key được lưu trữ trên Client - Ưu điểm: An toàn hơn so với SSH Password - Nhược điểm: Private Key cần được lưu trữ trên các thiết bị được dùng để đăng nhập vào Server

SSH

SSH Key hoạt động như thế nào? Tìm hiểu về SSH Key.

- Một cặp SSH Key: Public Key và Private Key.
- Thông tin của Public Key sẽ được lưu trữ trong **~/.ssh/authorized_keys**
- Public Key được dùng để mã hóa dữ liệu, và dữ liệu đó sẽ được giải mã bởi Private Key của người dùng

SSH

Kết nối SSH tới Server:

ssh <username>@<ip_server>

VD: `ssh toe@192.168.1.125`

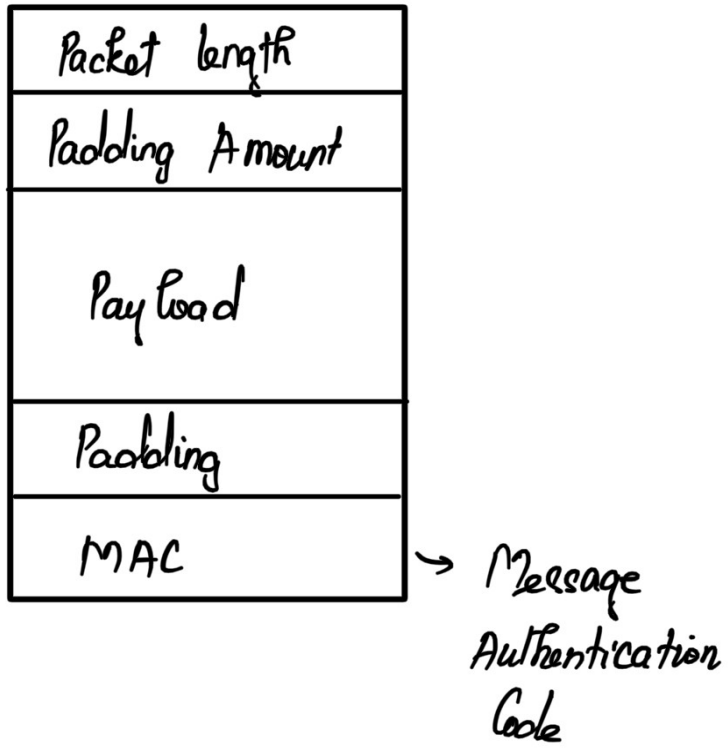
Nếu cổng kết nối khác 22, thì sử dụng tham số -p:

ssh -p <port> <username>@<ip_server>

VD: `ssh -p 2000 toe@192.169.1.125`

SSH

SSH hoạt động như thế nào?



SSH chia dữ liệu thành nhiều gói tin.

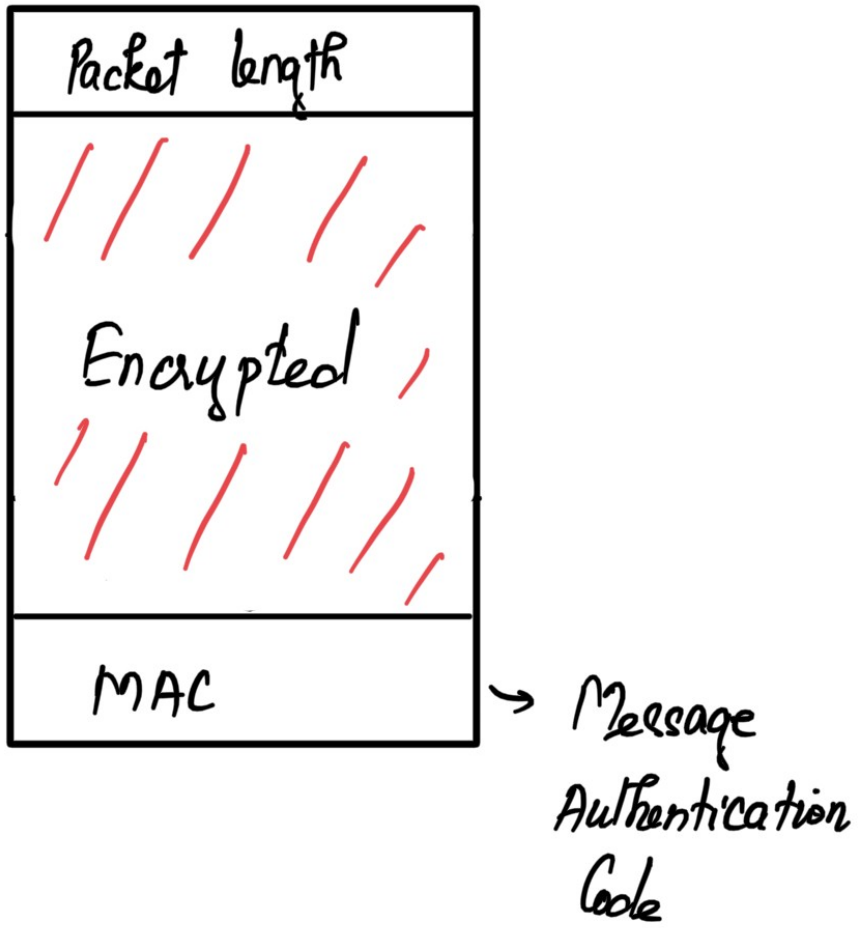
Packet Length: cho biết dung lượng của gói t
Padding Amount: cho biết có bao nhiêu phầ
đệm.
Payload: dữ liệu.
Padding: là các byte ngẫu nhiên
Message Authentication Code: để có thể ch
chắn dữ liệu chưa bị giả mạo.

SSH

SSH hoạt động như thế nào?

Payload cũng có thể được nén bằng các thuật toán nén tiêu chuẩn.

Packet sau đó được gửi đến server. Server giải mã gói tin và giải nén payload để trích xuất dữ liệu.



Các kỹ thuật mã hóa trong SSH

Để giữ an toàn cho SSH, SSH sử dụng ba loại kỹ thuật thao tác dữ liệu khác nhau tại các điểm khác nhau trong quá trình truyền.

Ba kỹ thuật được sử dụng trong SSH là:

- Symmetrical Encryption
- Asymmetrical Encryption
- Hashing

Các kỹ thuật mã hóa trong SSH

Để giữ an toàn cho SSH, SSH sử dụng ba loại kỹ thuật thao tác dữ liệu khác nhau tại các điểm khác nhau trong quá trình truyền.

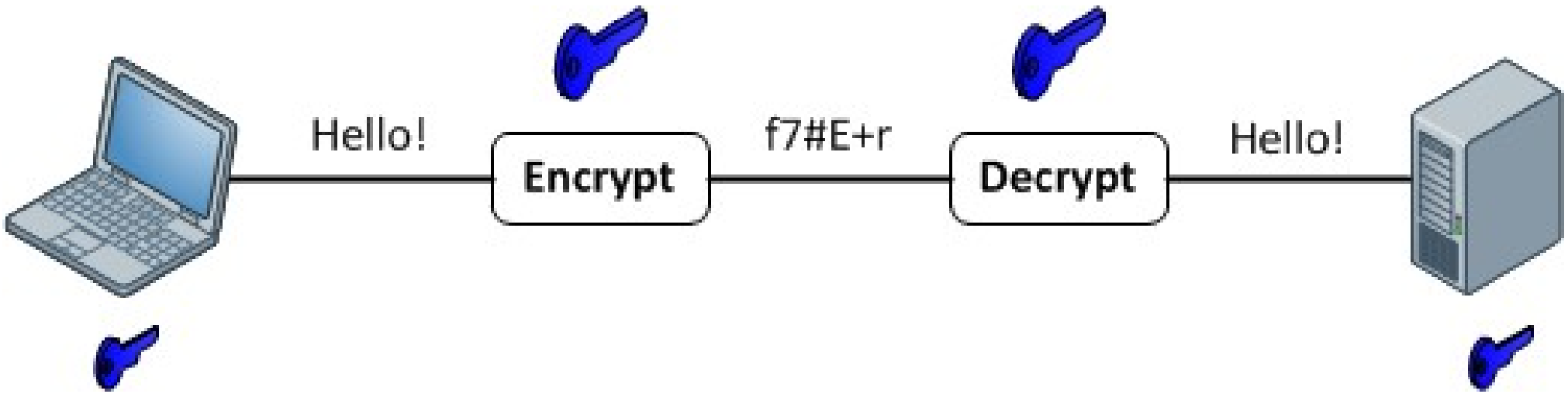
Ba kỹ thuật được sử dụng trong SSH là:

- Symmetrical Encryption
- Asymmetrical Encryption
- Hashing

Các kỹ thuật mã hóa trong SSH

Symmetrical Encryption (Mã hóa đối xứng)

Symmetrical encryption là loại mã hóa trong đó chỉ có một khóa (**secret key**) được sử dụng để vừa mã hóa vừa giải mã thông tin ở cả trên client và server.



Các kỹ thuật mã hóa trong SSH

Asymmetrical Encrytion (Mã hóa bất đối xứng)

Là một phương thức mã hóa không đối xứng được sử dụng trong SSH để bảo vệ đăng nhập và xác thực người dùng.

Hashing: Dùng để bảo đảm tính toàn vẹn trong quá trình truyền tải và xác thực

Thực hành: Sử dụng SSH Key

Bước 1: Tạo SSH Key: **ssh-keygen**

Nơi lưu trữ key. Private key Sẽ được gọi là id_rsa còn Public key là id_rsa.pub, cả 2 được lưu vào thư mực ~/.ssh

Bước 2: Copy SSH Public Key cho Server

Sử dụng: **ssh-copy-id toe@192.168.1.125**

Tự động kết nối tới tài khoản và copy Key public ~/.ssh/id_rsa.pub vào file trên server ~/.ssh/toe/authorized_keys/

Bước 3: Xác thực bằng SSH Key: Có thể đăng nhập vào Server mà không cần dùng mật khẩu

Thực hành: Thay đổi Port

Bước 1: Sửa tệp cấu hình SSH thông qua tệp **/etc/ssh/sshd_config**

```
sudo vi /etc/ssh/sshd_config
```

Bước 2: Tìm dòng #Port 22, bỏ dấu # sửa thành cổng mong muốn, ví dụ: Port 2345

Bước 3: Lưu tệp và khởi động lại dịch vụ SSH:

```
sudo service ssh restart
```

Bước 4: Sau khi thay đổi, để kết nối với máy chủ: **ssh -p 2345 toe@192.168.1.100**