Bài 16. An ninh hệ thống

An ninh cần được quan tâm khi cài đặt, triển khai, và sử dụng hệ thống. Mặc dù bản cài đặt mới Ubutun tương đối an toàn, hiểu về an ninh hệ thống sẽ được sử dụng sau khi triển khai và trong thời gian vận hành.

1. An ninh trong quản trị người dùng

Tài khoản Root

Vì lý do an ninh, tài khoản root được vô hiệu hóa theo mặc định trong các bản cài đặt Ubuntu. Điều đó không có nghĩa là tài khoản root đã bị xóa và không còn dùng được nữa. Đơn giản chỉ là tài khoản root đã được cấp một mật khẩu mà các mã hóa thông thường không thể tạo ra.

Người dùng được khuyến cáo sử dụng các công cụ với tiền tố sudo để thực hiện các tác vụ quản trị. Sudo cho phép người dùng có quyền tạm thời nâng quyền của họ để thực hiện các lệnh thuộc quyền root. Nếu vì lý do gì đó cần kích hoạt tài khoản root, đơn giản hãy cho root một mật khẩu.

```
sudo passwd

[sudo] password for username: (enter your own password)

Enter new UNIX password: (enter a new password for root)

Retype new UNIX password: (repeat new password for root)

passwd: password updated successfully
```

Để vô hiệu hóa sử dụng tài khoản root, chạy lệnh sau:

```
sudo passwd -l root
```

Tuy nhiên, để vô hiệu hóa chính tài khoản root, chạy lệnh sau:

```
usermod --expiredate 1
```

Theo mặc đinh, tài khoản được khởi tạo khi cài đặt Ubuntu là thành viên của nhóm “sudo” và được thêm vào tệp /etc/sudoers. Để một người dùng có quyền sudo, hãy đưa người dùng vào nhóm sudo.

An ninh với User Profile

Khi một người dùng được tạo, lệnh adduser sẽ tạo thư mục home cho người dùng với tên là /home/username, và profile mặc định được sao chép từ thư mục /etc/skel. Thư mục /home/username có quyền mặc định là rwxr-xr-x. Điều đó có nghĩa là người dùng bất kỳ đều có thể xem và thực thi trên thư mục /home/username. Để điều đó không xảy ra, hãy thay đổi quyền cho thư mục /home/username để chỉ người dùng username có quyền.

```
sudo chmod 0750 /home/username
```

Một cách tiếp cận hiệu quả hơn để thiết lập quyền trên các thực mục home của người dùng mới tạo là sửa đổi tệp /etc/adduser.conf với tham số DIR_MODE bằng quyền mong muốn.

```
DIR_MODE=0750
```

Chính sách mật khẩu

Sử dụng mật khẩu mạnh là biện pháp đơn giản nhưng quan trọng để đảm bảo an ninh hệ thống. Sử dụng mật khẩu mạnh để chống dò mật khẩu bằng các tấn công từ điển hay tấn công brute force. Mật

khẩu mạnh được thể hiện ở độ dài tối thiểu, độ phức tạp và thời gian hợp lệ của mật khẩu.

Mặc định Ubuntu sử dụng mật khẩu có độ dài tối thiểu là 6. Có thể tăng độ dài tiếu thiểu bằng cách sửa đổi minlen trong tệp /etc/pam.d/common-password như sau:

password [success=1 default=ignore] pam_unix.so obscure sha512 minlen=8

Để xem thời gian hợp lệ (age) của mật khẩu, sử dụng lệnh chage như sau:

sudo chage -l username

Kết quả được đưa ra màn hình có dạng:

Last password change : Jan 20, 2015

Password expires : never

Password inactive : never

Account expires : never

Minimum number of days between password change : 0

Maximum number of days between password change : 99999

Number of days of warning before password expires : 7

Sử dụng lệnh chage để thay đổi các tham số ngày tài khoản hết hạn (-E), số ngày tối thiểu (-m)/tối đa (-M) cần thay đổi mật khẩu, số ngày không đổi mật khẩu sau hạn dẫn đến tài khoản bị vô hiệu hóa (-I), và số ngày trước khi mật khẩu hết hạn được thông báo (-W) như ví dụ sau:

sudo chage -E 01/31/2015 -m 5 -M 90 -I 30 -W 14 username

Truy cập SSH bởi người dùng đã vô hiệu hóa

Người dùng đã vô hiệu hóa vẫn có thể truy cập từ xa bằng SSH nếu SSH sử dụng phương thức xác thực theo khóa. Nhớ bỏ khóa của những người dùng không được phép khỏi tệp /home/username/.ssh/authorized_keys. Xóa hay thay đổi thư mục .ssh của người dùng đã bị vô hiệu hóa để người dùng không thể truy cập bằng SSH nữa.

2. Vô hiệu hóa Ctrl+Alt+Delete

Tổ hợp Ctrl+Alt+Delete sẽ khởi động lại hệ thống. Để vô hiệu hóa tổ hợp này, chạy các lệnh sau:

```
sudo systemctl mask ctrl-alt-del.target

sudo systemctl daemon-reload
```

3. eCryptfs

eCryptfs là hệ thống tệp được mã hóa cho Linux. Được cài đặt ở tầng trên của hệ thống tệp, eCryptfs bảo vệ các tệp bất kể hệ thống tệp phía dưới là gì (NTFS, EXT, FAT,…).

Mục này mô tả ví dụ mã hóa thư mục /srv sử dụng eCryptfs.

Đầu tiên, cài đặt eCryptfs bằng cách chạy lệnh sau:

```
sudo apt install ecryptfs-utils
```

Tiếp theo, mount phân vùng được mã hóa bằng chạy lệnh sau, lưu ý có tùy chọn –t ecryptfs:

```
sudo mount -t ecryptfs /srv /srv
```

và cung cấp một số thông tin chi tiết về cách thức mã hóa.

Để kiểm thử, hãy chép một thư mục nào đó vào /srv, ví dụ:

```
sudo cp -r /etc/default /srv
```

unmount /srv, và cố gắng xem nội dung một tệp:

```
sudo umount /srv
cat /srv/default/cron
```

Mount lại /srv để thấy ecryptfs cho phép đọc nội dung /srv.

4. Tường lửa

Giới thiệu

Nhân Linux bao gồm hệ thống lọc gói tin Netfilte. Hệ thống này được sử dụng để quản lý các lưu lượng mạng đến hoặc đi qua máy chủ. Tất cả các tường lửa hiện đại cho Linux đều sử dụng hệ thống con này để lọc các gói tin.

Hệ thống lọc gói tin Netfilte sẽ ít được dùng bởi người quản trị nếu không có giao diện người dùng để tương tác với nó. iptables cung cấp giao diện như vậy để quản trị viên cung cấp luật (rules) cho Netfilte. Do vậy, iptables là tất cả những gì cần để quản trị tường lửa. Tuy nhiên, sử dụng iptables chưa thật sự đơn giản và cần có một frontends đơn giản hơn.

ufw - Uncomplicated Firewall

Frontend cho tường lửa trên Ubuntu là ufw. ufw cung cấp giao diện thân thiện với người dùng cho việc cấu hình tường lửa. ufw dược cài đặt nhưng bị vô hiệu hóa theo mặc định. Để kích hoạt ufw, chạy lệnh sau:

```
sudo ufw enable
```

Cấu hình tường lửa bằng các lệnh có dạng như sau:

Cho truy cập cổng:

```
sudo ufw allow 22
```

Cấm truy cập cổng:

```
sudo ufw deny 22
```

Bỏ luật:

```
sudo ufw delete deny 22
```

Cho truy cập từ một IP/mạng cụ thể đến mộc cổng:

```
sudo ufw allow proto tcp from 192.168.0.2 to any port 22
```

```
sudo ufw allow proto tcp from 192.168.0.0/24 to any port 22
```

Xem trạng thái của tường lửa:

```
sudo ufw status

sudo ufw status verbose
```

Tích hợp ufw vào ứng dụng

Ứng dụng mở cổng có thể bao hàm hồ sơ ufw. Hồ sơ được lưu trong thư mục /etc/ufw/applications.d. Hồ sơ cho một ứng dụng có dạng:

```
[TênHS]

title=Tiêu đề của ứng dụng

description=Mô tả về ứng dụng

porst=port/prot
```

trong đó, port là số hiệu cổng như 80, 22; prot là tên giao thức tầng giao vận (tcp/udp)

Để biết ứng dụng nào đã cài đặt hồ sơ, chạy lệnh sau:

```
sudo ufw app list
```

Khi đã có hồ sơ, có thể cấu hình lọc lưu lượng theo tên hồ sơ ứng dụng, ví dụ:

```
sudo ufw allow Samba
```

hoặc

```
ufw allow from 192.168.0.0/24 to any app Samba
```

Để xem chi tiết về hồ sơ cho một ứng dụng, ví dụ Samba, chạy lệnh sau:

```
sudo ufw app info Samba
```

Logs

Logs là thông tin thiết yếu để phát hiện tấn công, xử lý sự cố. Các luật ghi log của tường lửa phải được đặt trước các luật kết thúc như ACCEPT, DROP, hoặc REJECT.

Có thể bật/tắt chức năng ghi log của tường lửa bằng lệnh:

```
sudo ufw logging on|off
```

5. Chứng thư

Mật mã khóa công khai, còn gọi là mật mã khóa bất đối xứng, được sử dụng rộng rãi ngày nay. Các hệ thống mã hóa thông tin bằng khóa công khai (public key). Thông tin chỉ có thể giải mã bằng khóa bí mật (private key).

Secure Socket Layer (SSL) hoặc Transport Layer Security (TLS) là giao thức tầng 4.5, nằm giữa tầng 4 (giao vận) và tầng 5 (ứng dụng) giúp mã hóa và giải mã dữ liệu của ứng dụng mạng theo mật mã khóa công khai. Ví dụ, với lược đồ HTTPS, các gói tin HTTP được mã hóa bằng SSL trước khi gửi, và giải mã bằng SSL bên nhận.

Chứng thư (Certificate) là một phương thức được sử dụng để phân phối khóa công khai và những thông tin khác kèm theo như server và tổ chức có trách nhiệm về chứng thư. Chứng thư có thể được ký số bởi CA (Certification Authority). CA là đối tác thứ ba tin cậy có chức năng xác nhận thông tin trong chứng thư là chính xác.

Các loại chứng thư

Để thiết lập một server an toàn sử dụng mật mã khóa công khai, trong hầu hết các trường hợp, đơn vị sử dụng server gửi yêu cầu chứng thư (bao gồm khóa công khai), chứng minh định danh của tổ chức và trả tiền cho CA. CA xác minh yêu cầu và định danh của đơn vị. Theo một cách khác, đơn vị có thể tự tạo và sử dụng các chứng thư tự ký. Lưu ý không nên sử dụng chứng thư tự ký trong môi trường sản xuất. Ví dụ, nếu trình duyệt nhận được một chứng thư nhưng không nhận diện được CA, trình duyệt sẽ hỏi người dùng chấp nhận hay từ bỏ kết nối.

Các bước tạo và yêu cầu chứng thư như sau:

- Tạo cặp khóa công khai và bí mật.
- Tạo yêu cầu chứng thư dựa vào khóa công khai. Yêu cầu chứng thư bao gồm thông tin về server và công ty.
- Gửi yêu cầu chứng thư cho CA
- Nhận chứng thư từ CA (sau khi trả tiền)
- Cài đặt chứng thư vào server và cấu hình các ứng dụng trên server dùng chứng thư.

Tạo Certificate Signing Request (CSR)

Nếu cần thuê chứng thư từ CA hoặc tự tạo chứng thư tự ký, bước đầu tiên là tạo khóa.

Tạo khóa có thể sử dụng passphrase để tăng tính an toàn cho hệ thống.

Để tạo khóa cho Certificate Signing Request (CSR), chạy lệnh sau:

```
openssl genrsa -des3 -out server.key 2048
```

Nhập passphrase cho server.key. Lưu ý passphrase phân biệt ký tự hoa thường và càng dài, phức tạp càng an toàn.

Nhập lại passphrase.

Nếu tạo khóa không cần passphrase thì chạy lệnh sau. Lưu ý, khóa không có passphrase không an toàn bằng khóa có passphrase.

```
openssl rsa -in server.key -out server.key.insecure

mv server.key server.key.secure

mv server.key.insecure server.key
```

Để tạo CSR, chạy lệnh sau:

```
openssl req -new -key server.key -out server.csr
```

Nhập passphrase và các thông tin theo yêu cầu. Khi đã nhập đủ thông tin, CSR được tạo và lưu trong tệp server.csr.

Bây giờ có thể gửi server.csr đến CA. CA sử dụng server.csr để cấp chứng thư. Mặt khác, có thể tự tạo chứng thư tự ký từ CSR.

Tạo chứng thư tự ký

Để tạo chứng thư tự ký, chạy lệnh sau:

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

Nhập passphrase. Chứng thư được tạo và lưu thành tệp server.crt.

Lưu ý, nếu server được sử dụng trong môi trường sản xuất, không nên sử dụng chứng thư tự ký mà nên dùng chứng thư do CS cấp.

Cài đặt chứng thư

Để cài đặt khóa server.key và chứng thư server.crt, chạy lệnh sau:

```
sudo cp server.crt /etc/ssl/certs

sudo cp server.key /etc/ssl/private
```

Bây giờ có thể sử dụng chứng thư với các ứng dụng trên máy chủ.