XX. Thực hành cấu hình bảo mật truy cập SSH cho một Linux Server

Mở ứng dụng terminal của bạn và truy cập vào Linux Centos của bạn.

- **Lưu ý**: Để thực hiện bài thực hành này cần phải disable SELinux.

  ssh root@<YOUR_IP>

- Nhập mật khẩu của bạn tại dấu nhắc.

1. Cấu hình sshd để sử dụng Sockets.

- Xác minh là sshd.socket unit chưa được bật lên enable trong hệ điều hành.
  systemctl status sshd.socket
- Setup một at job để dừng dịch vụ sshd.service và khởi động sshd.socket.
  sudo at now + 3 minutes
- Nhập mật khẩu của bạn tại dấu nhắc. Thêm nội dung sau:
  at> systemctl stop sshd.service
  at> systemctl start sshd.socket
- Nhấn Ctrl + D để kết thúc việc cấu hình at.

- Xác nhận là sshd.socket unit đã được kích hoạt và đang chạy.
  systemctl status sshd.socket
- Cho phép enable sshd.socket được bật lên vĩnh viễn và tắt disable dịch vụ sshd.service.
  sudo systemctl enable sshd.socket
  sudo systemctl disable sshd.service

2. Cài đặt và cấu hinh sử dụng TCP wrappers trên Centos 8 :

- Cài đặt gói epel-release từ kho lưu trữ EPEL (Extra Packages for Enterprise Linux). Để có thể truy cập vào các gói phụ trợ và bổ sung từ kho lưu trữ EPEL trên CentOS/RHEL:

  dnf install epel-release

- Cài đặt gói tcp_wrappers, một công cụ cho phép bạn kiểm soát quyền truy cập các dịch vụ mạng:

  dnf install tcp_wrappers

- Copy file dịch vụ sshd@.service vào /etc/systemd/system/ :

cp /usr/lib/systemd/system/sshd@.service /etc/systemd/system/

3. **Tiếp theo chúng ta soạn thảo file "sshd@.service" để cho phép TCP wrappers quản lý dịch vụ ssh server:**

   vi /etc/systemd/system/sshd@.service

- Thay đổi dòng cấu hình" ExecStart=-/usr/sbin/sshd -i $OPTIONS $CRYPTO_POLICY " thành như sau:

  ExecStart=@-/usr/sbin/tcpd /usr/sbin/sshd -i $OPTIONS $CRYPTO_POLICY

- Thiết lập TCP Wrappers để chỉ cho phép truy cập từ xa vào SSH.Chỉnh sửa file /etc/hosts.allow:

  sudo vim /etc/hosts.allow

- **Thêm dòng sau vào file:**

  sshd2 sshd: ALL

- Chỉnh sửa file /etc/hosts.deny.

  sudo vim /etc/hosts.deny

- Thêm dòng sau vào file:

  ALL: ALL

- Thoát khỏi phiên SSH.

  exit

- Kết nối lại với phiên secure shell.

  ssh root@your_IP

- Nhập mật khẩu của bạn tại dấu nhắc.

- Như vậy Bài thực hành này cung cấp hướng dẫn về cách sử dụng TCP Wrappers và systemd socket để cấu hình bảo mật cho SSH trên CentOS. TCP Wrappers là một công cụ được sử dụng để giới hạn truy cập vào các dịch vụ mạng bằng cách cho phép hoặc từ chối các kết nối dựa trên địa chỉ IP hoặc hostname. Systemd socket là một cơ chế kích hoạt các dịch vụ mạng khi được yêu cầu, giúp tiết kiệm tài nguyên hệ điều hành, Vậy các bạn hãy thực hành một vài lần theo hướng dẫn để chúng ta hiểu được kiến thức tốt hơn.