XIX. Thực hành tạo sudo Users mới

1. Tạo hai người dùng mới

- Tạo một người dùng webuser trên hệ thống Linux:

  sudo useradd -m webuser

- Tạo một người dùng webadmin , và gán user này vào nhóm wheel:

  sudo useradd -G wheel -m webadmin

- Đặt mật khẩu cho cả hai tài khoản là Git12345!:

  sudo passwd webuser

  sudo passwd webadmin

- Xác nhận file /etc/sudoers Và Kiểm Tra quyền Truy Cập
- Xác nhận là file /etc/sudoers sẽ cho phép nhóm wheel có quyền chạy tất cả các lệnh với lệnh sudo:

  sudo visudo

- **Lưu ý**: không để một chú thích (#) comment trên dòng này của file:

  %wheel ALL=(ALL) ALL

- Chuyển sang tài khoản webadmin và sử dụng dấu gạch ngang (-) để sử dụng một login shell:

  sudo su - webadmin

- Thử test bằng cách Chạy lệnh đọc file /etc/shadow trong terminal:

  cat /etc/shadow

- Chạy lại lệnh với lệnh sudo:

  sudo cat /etc/shadow

- Sau khi xác minh là user webadmin có thể đọc được file /etc/shadow, đăng xuất ra khỏi tài khoản này:

  exit

2. Thiết lập user có quyền Quản trị dịch vụ Web

- Tạo một file sudoers mới trong thư mục /etc/sudoers.d :

  sudo visudo -f /etc/sudoers.d/web_admin

- Thêm 1 nội dung vào file, để cấp quyền cho người dùng quản trị dịch vụ web như sau:

Cmnd_Alias WEB = /bin/systemctl restart httpd.service, /bin/systemctl reload httpd.service

- Thêm một dòng khác vào file cho user webuser có thể sử dụng lệnh sudo kết hợp với bất kỳ lệnh nào được liệt kê trong nhóm alias WEB:

    webuser ALL=WEB

- Lưu và đóng file bằng lệnh :wq.

3. Tiếp theo, đăng nhập vào HĐH bằng tài khoản webuser:

sudo su - webuser

- Khởi động lại dịch vụ web:

  sudo systemctl restart httpd.service

- Thử đọc file sudoers mới tạo là web_admin:

  sudo cat /etc/sudoers.d/web_admin

- Do lệnh cat không được liệt kê trong dòng lệnh alias của file web_admin, vì vậy user webuser không thể sử dụng sudo để đọc file này.