Câu lệnh trong ubuntu Linux

User

* Nhóm lệnh thực thi:
  + sudo adduser (tennguoidung) : Thêm mới người dùng
  + sudo usermod -aG sudo (tennguoidung) : Thêm mới người dùng vào nhóm sudo
  + sudo useradd -m -s /bin/bash (username) : Tạo tài khoản không cần thông tin bổ sung
    - - m : Tạo thư mục home
    - - s : Chỉ định shell (mặc định là /bin/bash)
  + sudo deluser (username) : xóa tài khoản
  + sudo deluser --remove-home (username) : xóa tài khoản và thư mục home
  + sudo usermod -l new\_username old\_username : đổi tên tài khoản
    - sudo usermod -d /home/new\_username -m new\_username : đổi cả thư mục home
  + sudo usermod -s /bin/zsh (username) : Thay đổi shell đăng nhập
  + Mở/Khóa tài khoản:
    - sudo usermod -L (username) : Khóa tài khoản
    - sudo usermod -U (username) : Mở khóa tài khoản
  + Thay đổi mật khẩu:
    - Passwd
    - sudo passwd username : thay đổi mật khẩu cho người khác
  + Quản lý nhóm:
    - sudo groupadd groupname: Tạo mới nhóm
    - sudo groupdel groupname : Xóa nhóm
    - sudo usermod -aG groupname username : Thêm người vào nhóm
    - groups username : Xem người dùng thuộc nhóm nào
* Nhóm lệnh tra cứu:
  + awk -F: '$3 >= 1000 {print $1}' /etc/passwd : Danh sách người dùng thực không bao gồm hệ thống
  + cat /etc/passwd : Liệt kê danh sách người dùng
  + su – (tennguoidung): Kiểm tra đăng nhập bằng tài khoản mới
  + id (username) : xem quyền của user
  + ls -l /path/to/file\_or\_directory : xem quyền truy cập tập tin
  + groups (username) : Xem thông tin về nhóm
  + getent group sudo : kiểm tra quyền sudo
  + who : kiểm tra người dùng hiện tại đang đăng nhập
  + w : Hiển thị phiên đăng nhập đang hoạt động
  + last : Lịch sử đăng nhập
* Cấu hình:
  + Giới hạn thời gian đăng nhập: /etc/security/time.conf
  + Hạn chế tài nguyên người dùng: /etc/security/limits.conf
  + sudo chown username:groupname /path/to/directory : đổi chủ sỡ hữu đăng nhập
  + sudo usermod -g $(id -g olduser) -G $(id -G olduser | tr ' ' ',') newuser : sao chép quyền của người khác
  + sudo grep 'COMMAND=' /var/log/auth.log : Kiểm tra ai đang chạy lệnh sudo

Nginx

* Sử dụng systemctl:
  + sudo systemctl restart nginx : Khởi động lại
  + sudo systemctl status nginx : kiểm tra trạng thái

Firewall (Cấu hình tường lửa – UFW)

* sudo apt install ufw: Cài đặt UFW
* sudo ufw allow OpenSSH: 3 câu lệnh chỉ cho phép các kết nối cần thiết
* sudo ufw enable
* sudo ufw status

Cài đặt SSH (cấu hình SSH để an toàn hơn)

* sudo nano /etc/ssh/sshd\_config : Mở cấy hình SSH cấu hình những thuộc tính sau
  + PermitRootLogin no : Chỉ cho phép đăng nhập bằng tài khoản không phải root
  + PasswordAuthentication no : Cấm đăng nhập bằng mật khẩu nếu sử dụng (SSH Key)
  + Port 2200 : Thay đổi cổng mặc định nếu cần
* sudo systemctl restart sshd : Lưu và khởi động lại SSH
* Tạo SSH Key trên máy cục bộ
  + ssh-keygen
  + ssh-copy-id -i ~/.ssh/id\_rsa.pub tennguoidung@ip\_server
* Tạo ssh-Key thủ công
  + Sau khi dùng lệnh ssh-keygen
  + Trên win:
    - cat ~/.ssh/id\_rsa.pub : mở file chứa public key
    - ssh username@your-server-ip : đăng nhập vào server
    - Tạo thư mục .ssh nếu chưa có
      * mkdir -p ~/.ssh
      * chmod 700 ~/.ssh
    - echo "your-public-key-content" >> ~/.ssh/authorized\_keys : Thêm public key vào file authorized\_keys
    - chmod 600 ~/.ssh/authorized\_keys : đặt quyền cho authorized\_keys

Cài đặt Fail2Ban (Giúp bảo vệ server khỏi tấn công brute-force)

* sudo apt install fail2ban : Cài đặt
* Tùy chỉnh cấu hình: tạo file cấu hình tùy chỉnh
  + sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
  + sudo nano /etc/fail2ban/jail.local
* sudo systemctl enable --now fail2ban : Khởi động lại dịch vụ

Vô hiệu hóa các dịch vụ không cần thiết

* sudo systemctl list-units --type=service : Kiểm tra các dịch vụ đang chạy
* Tắt các dịch vụ không sử dụng:
  + sudo systemctl disable ten\_dich\_vu
  + sudo systemctl stop ten\_dich\_vu

Bật cập nhật tự động:

* sudo apt install unattended-upgrades
* sudo dpkg-reconfigure --priority=low unattended-upgrades

Cài đặt phần mềm bảo mật bổ sung:

* sudo apt install clamav: ClamAV quest virut
* Kiểm tra rootkits:
  + sudo apt install rkhunter
  + sudo rkhunter –checkall

Theo dõi nhật ký hệ thống:

* sudo journalctl -xe : sử dụng journalctl để theo dõi nhật ký

Kiểm tra trạng thái bảo mật: (sử dụng lynis)

* sudo apt install lynis : cài đặt
* sudo lynis audit system : chạy kiểm tra

Backup dữ liệu định kỳ:

* Sử dụng rsync hoặc cron để tự động sao lưu