**I. QUẢN LÝ NGƯỜI DÙNG VÀ MÁY TÍNH**

**1. Windows**

* Quản trị Users
* Có 4 loại user

**+** Administrators**:** Tài khoản sẽ có toàn quyền kiểm soát hệ thống.

**+** St**andard users:** Tài khoản này được cho phép đăng nhập vào máy tính, chạy ứng dụng, hiệu chỉnh thông tin tài khoản riêng. Người dùng sẽ bị hạn chế thực hiện thay đổi trên hệ thống.

**+** Child: Tài khoản dành cho trẻ nhỏ.

+ Guest: Tài khoản khách là tài khoản cho phép một người nào đó truy cập tạm thời vào máy tính của bạn và không được phép thực hiện bất kì thay đổi nào.

* Quản trị nhóm
* Mọi tài khoản Windows đều là thành viên của ít nhất một nhóm.
* Thành viên nhóm được xác định qua giấy phép mà chúng có.
* Đa số người dùng sử dụng những nhóm được tạo sẵn trong Windows, tuy nhiên chúng ta có thể tạo nhóm khác và tùy chỉnh cho nó. Thành viên nhóm được xác định qua giấy phép mà chúng có.

a) Tạo local account (tài khoản cho phép người dùng truy nhập vào máy tính cụ thể. Tài khoản này có giá trị với 1 máy tính duy nhất)

* Cách tạo Users
* Mở Computer Managerment
* Tạo user mới bằng cách: Users -> New User -> Nhập users -> Create
* Xóa user bằng cách: Users cần xóa -> Delete -> Yes
* Groups
* Mở Computer Managerment
* Tạo Group mới: Groups -> New Group -> Nhập group -> Create
* Add các user vào một Group: Group cần add -> Add to Group -> Add -> Nhập tên user cần add -> OK -> Apply -> Ok.

b) Với Domain account (Tài khoản được tạo trên máy chủ miền và được phép truy cập vào các tài nguyên của miền)

* Users
* Mở Server Manager -> Tool -> Active Directory User and Computer -> Chọn hoangtrungkien098.it -> New -> Organizational Unit -> Đặt tên là ptit -> ok
* Tạo user mới bằng cách: Users -> New User -> Nhập thông tin user -> Create
* Xóa user bằng cách: Users cần xóa -> Delete -> Yes
* Groups
* Tạo Group mới: Groups -> New Group -> Nhập group -> Create
* Add các user vào một Group: Group cần add -> Add to Group -> Add -> Nhập tên user cần add -> OK -> Apply -> Ok

**2. Linux (Ubuntu)**

* Quản trị Users
* Linux là hệ điều hành hỗ trợ nhiều người dùng.
* User trong Linux gồm user và super user (root)
* Mỗi user thường có đặc điểm như sau

+ Tên tài khoản user là duy nhất.

+ Mỗi user có 1 mã định danh duy nhất (uid).

+ Mỗi user có thể thuộc về nhiều group.

+ Tài khoản super user có uid=gid(mã định danh group)=0.

* **Một số thao tác với user**

**+** Thêm user mới: # sudo useradd -m *(tên user*)

+ Đặt mật khẩu cho user: # sudo passwd *(tên user)*

+ Thêm user vào một Group: # sudo usermod -a -G *(tên Group tên user)*

+ Thêm nhiều user vào 1 Group: # sudo gpasswd -M *(tên 1, tên 2, tênGroup)*

+ Xóa user khỏi 1 Group: # sudo gpasswd -d *(tên User, tên Group)*

+ Xóa user: # sudo userdel *(tên user)*

* **Quản trị group**
* Group là tập hợp của nhiều user.
* Mỗi group có 1 tên duy nhất và 1 mã định danh duy nhất (gid).
* Khi tạo ra 1 user (không dùng option -g) thì mặc định 1 group mang tên user được tạo ra.
* **Một số thao tác quản trị group**

+ Thêm Group mới: # sudo groupadd *(tên Group)*

+ Xóa Group: # sudo groupdel *(tên Group)*

+ Thay đổi tên Group: # sudo groupmod -n *Newname Oldname*

*+ nhóm các user vào group quản trị*

\*Ưu nhược điểm  
-Ubuntu

+ Đảm bảo an ninh và ngăn chặn phần mềm độc hại nhờ việc các ứng dụng chạy bằng tài khoản người dùng thông thường chứ không phải với đặc quyền quản trị hệ thống.

+ Trong trường hợp hệ thống cần cho nhiều người dùng, chỉ cần tạo thêm người dùng vào hệ thống.

+ Dễ dàng sao lưu các file của người dùng vì chúng được lưu bên trong thư mục riêng của từng người dùng.

* Windows:

+ Thực hiện việc quản trị phức tạp hơn.

+ Với mỗi tài nguyên có kiểm soát truy nhập người dùng có thể thực hiện hay cấp các quyền quản trị.

* **Kết luận:** Quản lý người dùng và máy tính trong 2 hệ điều hành Windows và Linux (Ubuntu) là tương đối giống nhau. Đều là hệ điều hành nhiều người dùng, dễ dàng tạo user và phân quyền truy nhập. Hỗ trợ nhiều chức năng quản trị máy tính cho người dùng. Tuy nhiên, ta thấy được hệ điều hành Ubuntu có phần linh hoạt và thuận tiện hơn Windows trong việc quản trị người dùng.

**II. SAO LƯU VÀ KHÔI PHỤC**

Sao lưu (Backup) dữ liệu là quá trình sao chép hoặc lưu trữ các tệp và thư mục.

Khôi phục (Restore) là một tính năng trong Microsoft Windows cho phép người dùng khôi phục lại trạng thái máy tính của họ về thời điểm trước đó đã sao lưu lại

1. **Windows**

* Một số ưu điểm nổi bật:

+ Thân thiện với người dùng

+ Thích hợp sao lưu và khôi phục đối với máy tính của cá nhân.

* Một số phương tiện sao lưu

+ Băng từ

+ Ổ đĩa quang

+ Ổ đĩa cứng

* Lựa chọn mục sao lưu

+ Tách biệt chương trình và dữ liệu

+ Áp dụng chính sách sao lưu khác nhau

* Một số phương pháp sao lưu:

+ Sao lưu dữ liệu trực tuyến. Dữ liệu được đọc hoặc phát trực tuyến từ máy chủ trực tiếp hoặc thông qua máy chủ dự phòng đến một phương tiện thứ cấp hoặc hệ thống lưu trữ nào đó.

+ Sao lưu dữ liệu vào ổ cứng hay thiết bị lưu trữ nào khác

* Một số chính sách sao lưu:

+ Sao lưu toàn bộ: Tạo bản sao toàn bộ file và dữ liệu

+ Sao lưu tăng dần Sao lưu toàn bộ tiếp theo là sao lưu tăng dần

+ Sao lưu khác biệt Sao lưu toàn bộ tiếp theo là sao lưu các file và dữ liệu khác biệt

* Cách cài đặt

+ Sử dụng chương trình “*Windows Server Backup*” - chương trình cho phép người quản trị lựa chọn các chính sách, loại file cũng như chương trình sao lưu khác nhau.

+ Người quản trị có thể chọn việc khôi phục được thực hiện vào dữ liệu được sao lưu.

* Kết quả:

1. **Hệ điều hành Linux**

* Đặc điểm: Hỗ trợ sao lưu và khôi phục bằng phương pháp câu lệnh và phương pháp đồ họa
* Một số ưu điểm nổi bật của Ubuntu:

+ Tính bảo mật cao

+ Có nhiều phần mềm và tính năng đa dạng

* Các loại backup:

+ Full backup: sao lưu toàn bộ các Files và Folder

+ Incremental backup: 1 xác lập để backup những file có sự thay đổi từ lần cuối backup cuối cùng.

+ Differential backup : 1 xác lập để backup những file có sự thay đổi từ lần cuối backup cuối cùng full backup

* Những công cụ hỗ trợ:

+ Tar

+ Sbackup

+ Bacular

+ ….

* Sao lưu và khôi phục bằng phần mềm:

+ Thông qua giao diện, người dùng có thể xác định nội dung cần được sao lưu cũng như thực hiện việc sao lưu tới các ổ đĩa cục bộ hay qua mạng.

+ Nội dung sao lưu còn có thể được bảo vệ qua việc sử dụng mật khẩu.

**Hình 1: Phần mềm sao lưu và khôi phục ở HĐH Ubuntu**

**Hình 2: Kết quả sau khi sao lưu vào file Picture**

**Hình 3 Những file đã sao lưu và sẵn sàng để khôi phục**

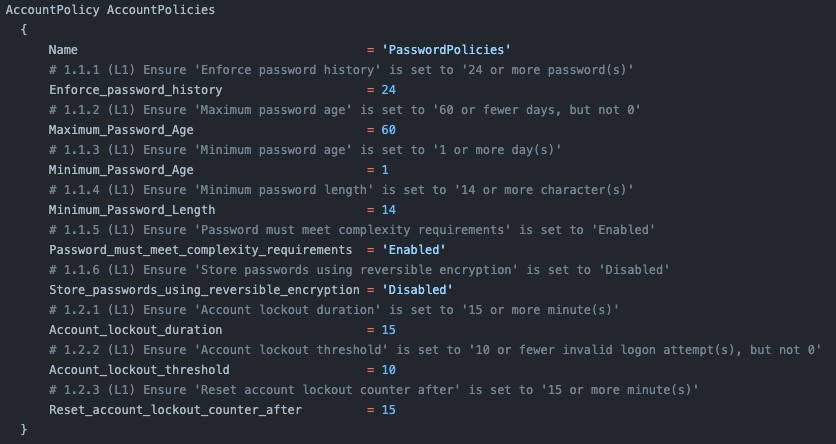
**III. TĂNG CƯỜNG AN NINH HỆ THỐNG (SYSTEM HARDENING)**

## Windows

* Sử dụng bài kiểm tra tính cứng của hệ thống bằng HardeningKitty

HardeningKitty hỗ trợ làm cứng hệ thống Windows. Cấu hình của hệ thống được truy xuất và đánh giá bằng cách sử dụng danh sách tìm kiếm. Ngoài ra, hệ thống có thể được cứng lại theo các giá trị được xác định trước. HardeningKitty đọc cài đặt từ sổ đăng ký và sử dụng các mô-đun khác để đọc cấu hình bên ngoài sổ đăng ký

* Để cài đặt làm tăng tính cứng của hệ thống một cách nhanh chóng ta có thể sử dụng các dòng lệnh cmd hay powershell. Trong bài này sử dụng một đoạn dòng lệnh mã nguồn mở ***github.com/NVISOsecurity/posh-dsc-windows-hardening***



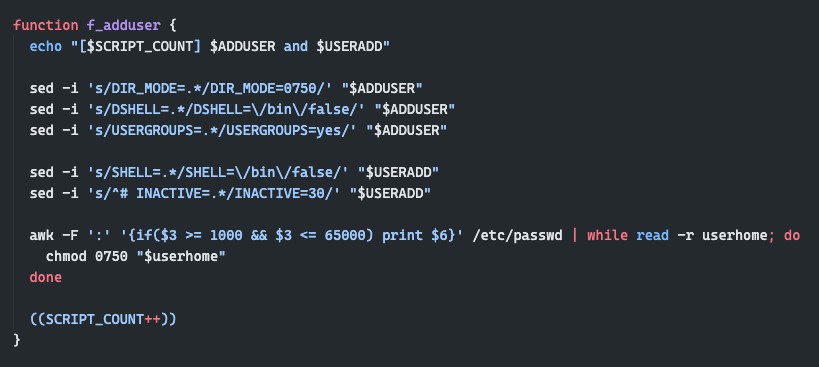
Ví dụ về cài đặt Chính sách tài khoản

## Linux

* Sử dụng bài kiểm tra tính cứng của hệ thống bằng Lynis

Lynis là một công cụ kiểm toán bảo mật cho các hệ thống dựa trên UNIX như Linux, macOS, BSD và các hệ thống khác. Nó thực hiện quét bảo mật chuyên sâu và chạy trên chính hệ thống

* Để cài đặt làm tăng tính cứng của hệ thống một cách nhanh chóng ta có thể sử dụng các dòng lệnh shell (sh hoặc bash). Trong bài này sử dụng một đoạn dòng lệnh mã nguồn mở ***github.com/konstruktoid/hardening.git***



Ví dụ về cài đặt thêm người dùng

* **Đánh giá trước (bên trái) và sau (bên phải) khi làm cứng hệ thống.**
* Làm cứng shell trên linux và powershell trên windows
* Làm cứng quá trình Khởi động và đăng nhập
* Làm cứng Tài khoản và người dùng

* Tường lửa và kiểm tra mã độc: Vì là một hệ điều hành đóng và phải trả phí nên windows có hệ thống tường lửa, và kiểm tra mã độc mặc định tốt hơn so với linux.
* Sau khi thực hiện làm cứng và kiểm tra lại các tiêu chí đánh giá

