



BÁO CÁO BÀI TẬP LỚN

# HỆ ĐIỀU HÀNH WINDOWS VÀ LINUX/UNIX

Nhóm D20N03G03

# Chủ đề tìm hiểu

1 ————— 2 ————— 3 ————— 4 ————— 5

CHIA SẺ  
FILE VÀ  
MÁY IN

Trần Quốc Huy.

QUẢN LÝ  
TRANG  
WEB

Lục Nguyễn  
Trang Nhi

QUẢN LÝ  
NGƯỜI  
DÙNG VÀ  
MÁY TÍNH

Lưu Văn Hưng

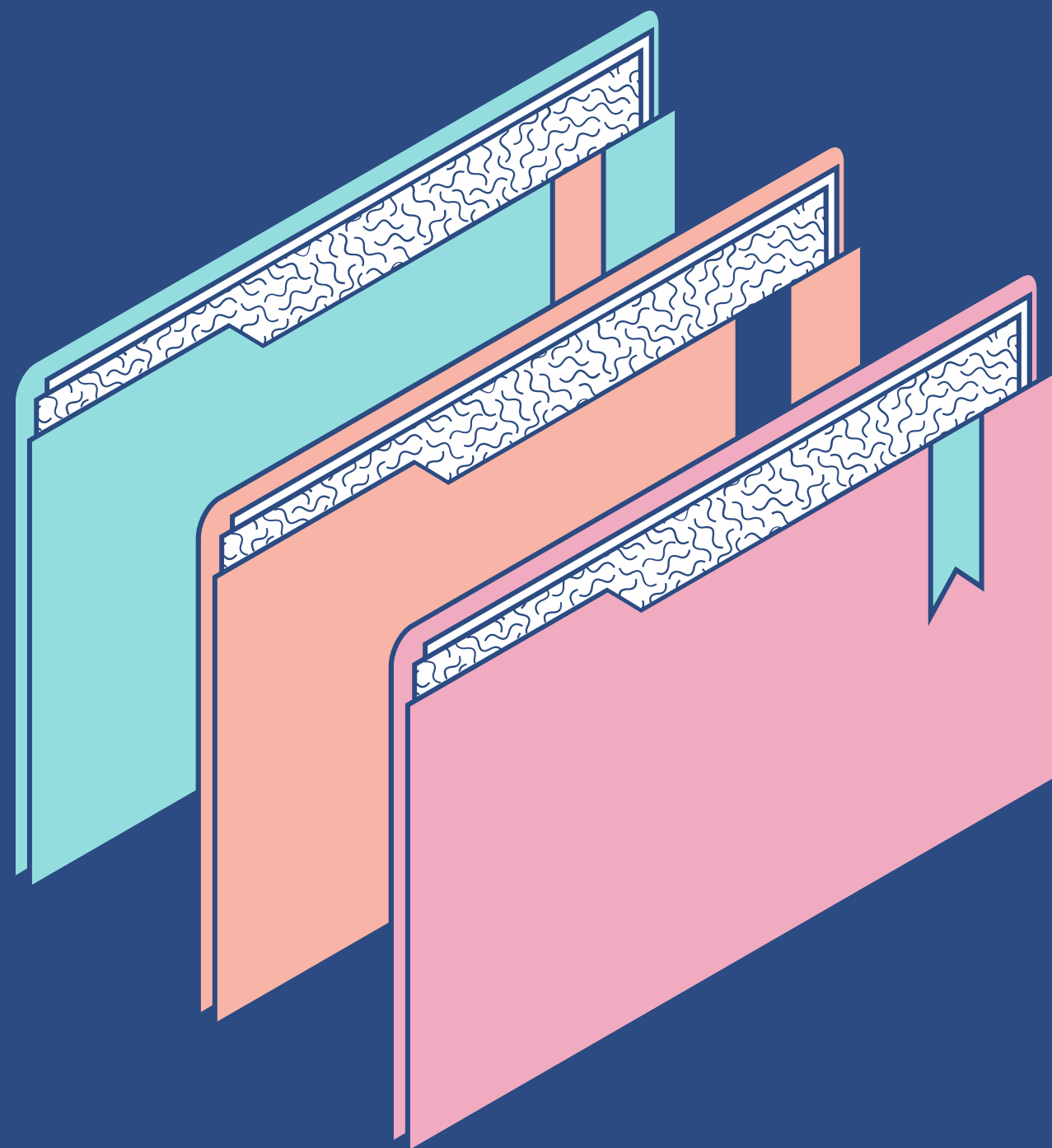
DỊCH VỤ  
TRUY  
NHẬP TỪ  
XA

Lại Quốc Đạt

GIÁM SÁT VÀ  
KIỂM TOÁN.  
TÌM HIỂU CÁC  
LOẠI LOG

Phạm Công  
Thước

SO SÁNH CÀI ĐẶT VÀ QUẢN TRỊ  
MỘT SỐ DỊCH VỤ CỦA HỆ ĐIỀU  
HÀNH WINDOWS VÀ LINUX



# Dịch vụ chia sẻ file và máy in

Dịch vụ file cho phép người dùng lưu trữ và chia sẻ các dữ liệu, chương trình với người dùng khác trong mạng.



# WINDOWS

Cung cấp công cụ cơ bản và đơn giản nhất để chia sẻ và quản lý.

Có thể hai hình thức đảm bảo an ninh:

- **Quyền với thư mục chia sẻ.** Hình thức này chỉ áp dụng với thư mục và các quyền của người dùng giới hạn: Đọc/Ghi/Sở hữu
- **Phân quyền NTFS** để kiểm soát việc truy nhập. Hình thức này cho phép giám sát tốt hơn và các quyền chi tiết hơn.

# LINUX

Giao thức truyền file FTP:

- Là giao thức cho phép tải các file giữa các máy tính nối mạng Internet, hoạt động ở cổng 20, 21 và có 2 chế độ kết nối: Nặc danh và Xác thực
- Cho phép truyền nhiều tin cùng 1 lúc, tự động chuyển tệp tin nếu mất kết nối và có khả năng đồng bộ hóa tệp tin

Dịch vụ NFS:

- Cho phép người sử dụng file/thư mục trên máy tính giống như trong ổ đĩa cục bộ. Theo mô hình client/server
- Máy chủ: chia sẻ thư mục. Máy khách: truy nhập thư mục chia sẻ trên máy chủ



# WINDOWS

- Yêu cầu đủ tốc độ mạng
- Phải giải quyết nhiều phân vùng cùng lúc và không gian bị lãng phí

# LINUX

FTP:

- Khả năng bảo mật kém.
- Máy chủ có khả năng bị qua mặt, gửi thông tin đến các cổng ngẫu nhiên.

NFS:

- Không an toàn, chỉ nên sử dụng trên 1 mạng đáng tin cậy sau Firewall.
- Bị chậm khi lưu lượng mạng lớn
- Client và server tin tưởng lẫn nhau hoàn toàn.



# WINDOWS

# LINUX

## Cài đặt

Thông qua trình quản lý máy in phù hợp

Định cấu hình thủ công bằng CUPS

Kết nối thông qua việc phát hành driver máy in của từng nhà sản xuất

## Quản trị

Tùy chỉnh và định cấu hình máy in

- Dễ dàng quản lý tài liệu và hoạt động in
- Khi gặp sự cố khó tìm được nguyên nhân

- Định cấu hình thủ công nên khó thao tác
- Do lưu được log nên dễ dàng quản lý tác vụ in

# Quản lý trang web

WEB LÀ HỆ THỐNG CÁC TÀI LIỆU DẠNG SIÊU VĂN BẢN LIÊN KẾT VỚI NHAU (TRANG WEB) MÀ NGƯỜI DÙNG CÓ THỂ XEM ĐƯỢC NHỜ TRÌNH DUYỆT.

Đối với hệ điều hành Windows dịch vụ Web được cung cấp thông qua dịch vụ thông tin IIS (Internet Information Services). Ngược lại đối với hệ điều hành Linux được cung cấp thông qua máy chủ Web Apache.





# Cài đặt quản lý trang web

## Windows

Sử dụng công cụ IIS, trong connections:

- Chọn vị trí cây site
- Đặt đường dẫn vật lý lưu trữ các file
- Đặt mật khẩu (nếu cần) xác định user
- Xác định địa chỉ IP trang web

Cách xác thực:

- Nặc danh (Anonymous)
- Xác thực cơ bản (Basic Authentication)
- Xác thực số (Digest Authentication)
- Xác thực Windows (Windows Authentication)

## Linux

Sử dụng Apache:

- Khởi tạo trang web

```
sudo a2ensite nhilnt.com.conf  
systemctl reload apache2
```

- Tắt địa chỉ web

```
sudo a2dissite nhilnt..com.conf  
systemctl reload apache2
```

- Tạo địa chỉ web ngầm định

Cách xác thực:

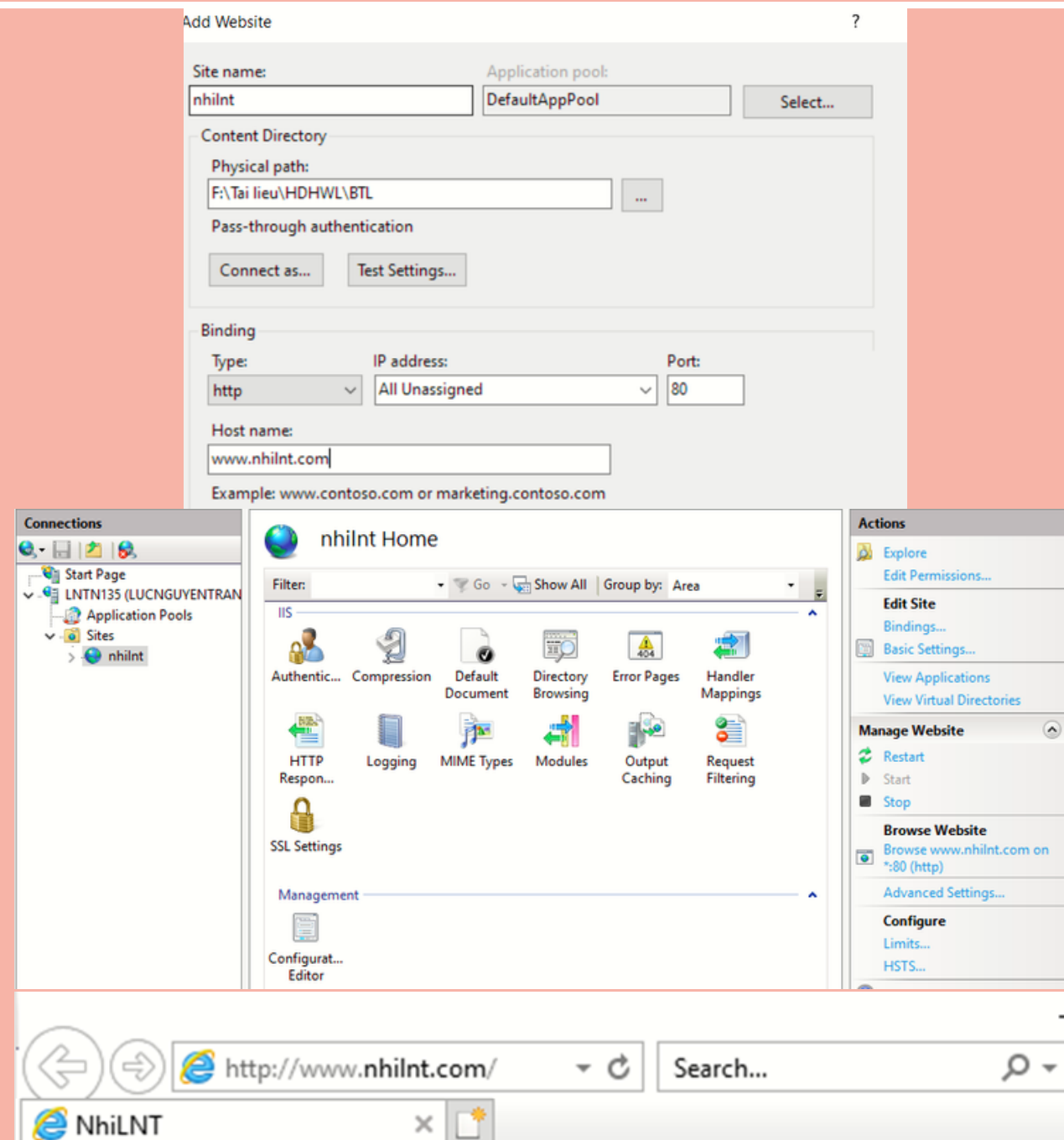
- Basic authentication
- Digest authentication



# Cài đặt quản lý trang web

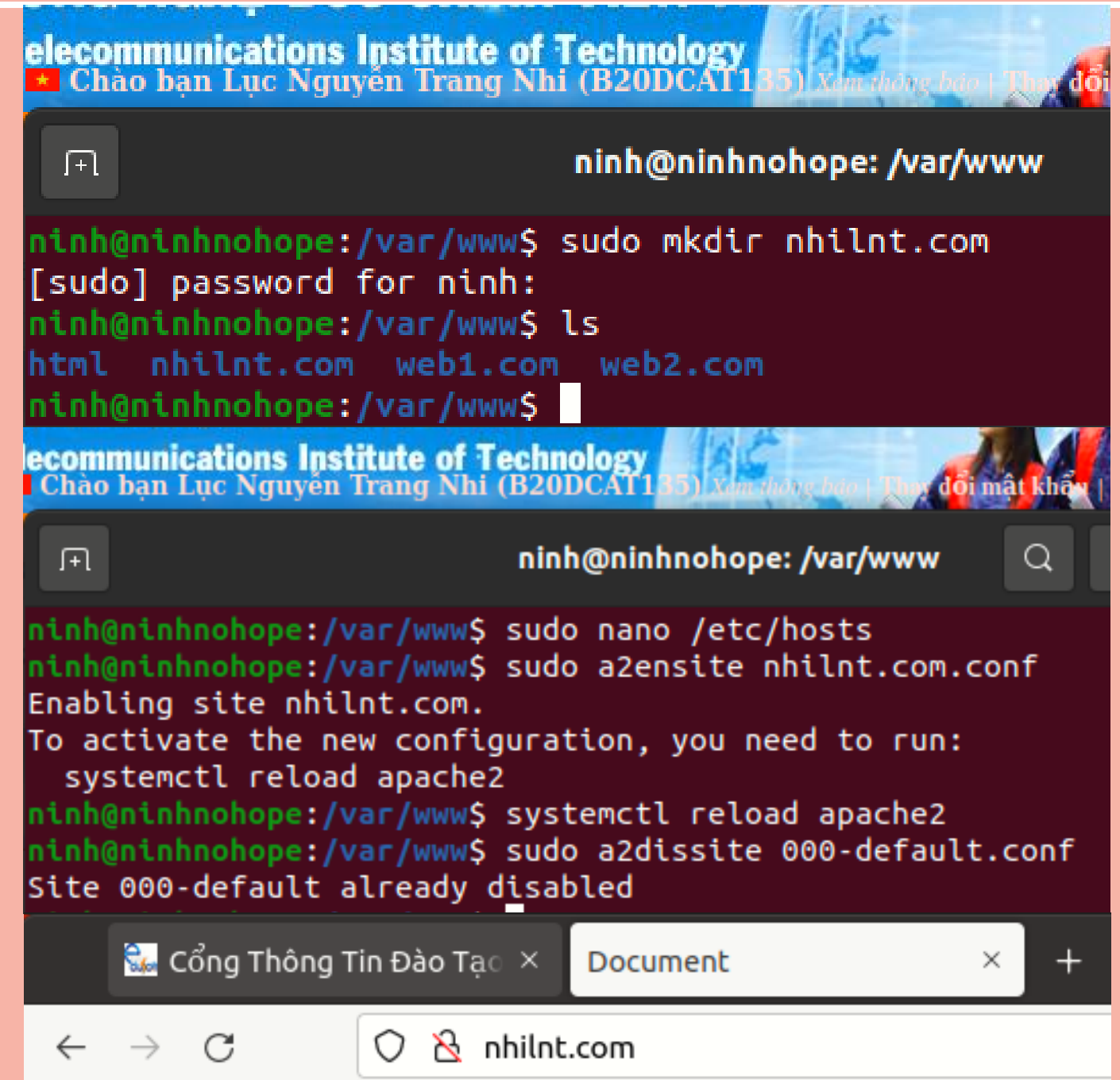
Tạo 1 trang web có nội dung “Hello LNTN” có địa chỉ nhilnt.com bằng Windows và Linux

## Windows



Hello LNTN

## Linux



Hello LNTN

## Windows

## Linux

### Ưu điểm

- Hoạt động trực quan, thân thiện với người dùng qua giao diện đồ họa
- Cập nhật hệ thống tự động hóa dễ dàng và tùy chọn.
- Hỗ trợ một số lượng lớn các ứng dụng của bên thứ ba

- Miễn phí, phần mềm mã nguồn mở, tính ổn định và an toàn,
- Hiếm khi lỗi bảo mật và thậm chí có thể dễ dàng xử lý chúng.
- Tích hợp chức năng từ xa

### Nhược điểm

- Chi phí cấp phép cao, chỉ chạy trên Windows.
- Thường gặp lỗi liên quan đến bảo mật. Dễ bị nhiễm phần mềm độc hại
- Sử dụng nhiều tài nguyên

- Hoạt động phức tạp
- Một số chương trình của bên thứ ba chỉ có thể cài đặt bởi quản trị viên

# Quản lý người dùng và máy tính

Mỗi người dùng cần có tài khoản người dùng riêng. Tài khoản được sử dụng khi người dùng đăng nhập mạng hay miền thư mục động



# WINDOWS



**Mỗi một người dùng có tài khoản người dùng riêng.**

- Việc quản trị chia tài khoản thành quản trị (Admin) và khách (Guest)
- Các người dùng có vai trò và yêu cầu tương tự nhau có thể được xếp vào cùng group

**Kiểm soát truy nhập người dùng các quyền tiêu biểu**

- Toàn quyền kiểm soát
- Sửa
- Đọc
- Ghi

# LINUX

**Người quản trị có thể sử dụng các câu lệnh thêm, bớt, sửa, xóa user và nhóm như sau:**

- useradd, userdel, usermod: nhóm lệnh quản lý người dùng
- groupadd, groupdel, groupmod: nhóm lệnh quản lý nhóm
- passwd: thay đổi mật khẩu người dùng.

**Người dùng có thể thay đổi quyền thông qua các lệnh chmod và chown**

- chown: thay đổi quyền sở hữu file hay thư mục
- chmod thay đổi quyền truy nhập file hay thư mục: #chmod [nhóm người dùng] [thao tác] [quyền hạn] [tập tin/thư mục]

Trong đó:

- Nhóm người dùng: u - user; g - group; o - others; a - all.
- Thao tác: "+" là thêm quyền; "-" là xóa quyền; "=" là gán quyền bằng
- Quyền: r - đọc; w - ghi; x - thực thi

## WINDOWS

## LINUX

### Giống nhau

- Đều là hệ điều hành nhiều người dùng nhưng có (Administrator hay Root) có quyền cao nhất
- Đều có chức năng tạo, sửa, xóa User, phân quyền truy nhập
- Cả Windows và Ubuntu đều cho phép chia sẻ, đọc ghi file trong một group.

### Khác nhau

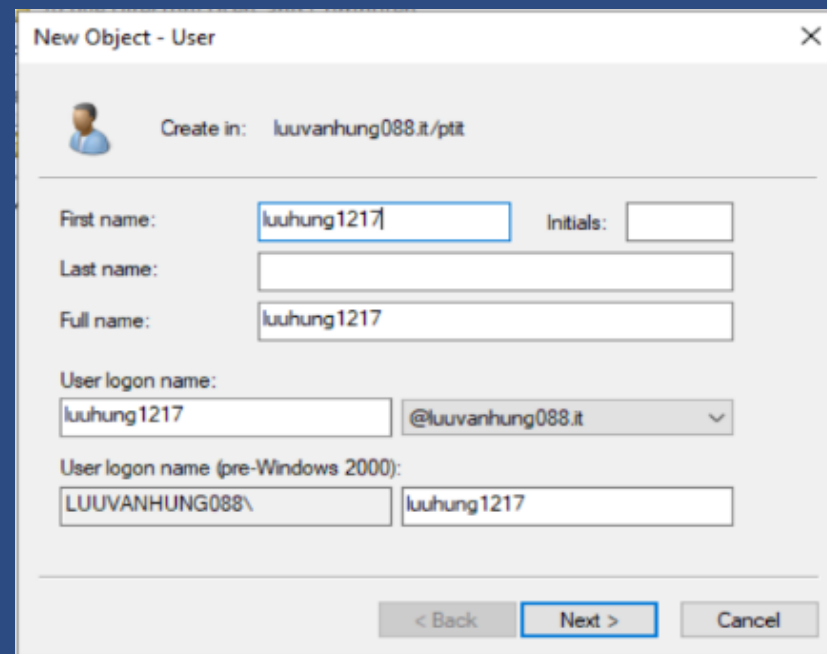
- Có thể dùng Guest để đăng nhập nếu không có tài khoản
- Thực hiện quản trị trên Computer Manager hay server Manager
- Trong Windows, nếu muốn chia sẻ file thì phải join vào cùng một domain

- Bắt buộc phải có tài khoản nếu muốn sử dụng
- Thực hiện quản trị bằng các dòng lệnh trên Terminal
- Phân quyền file thông qua terminal 1 cách nhanh chóng

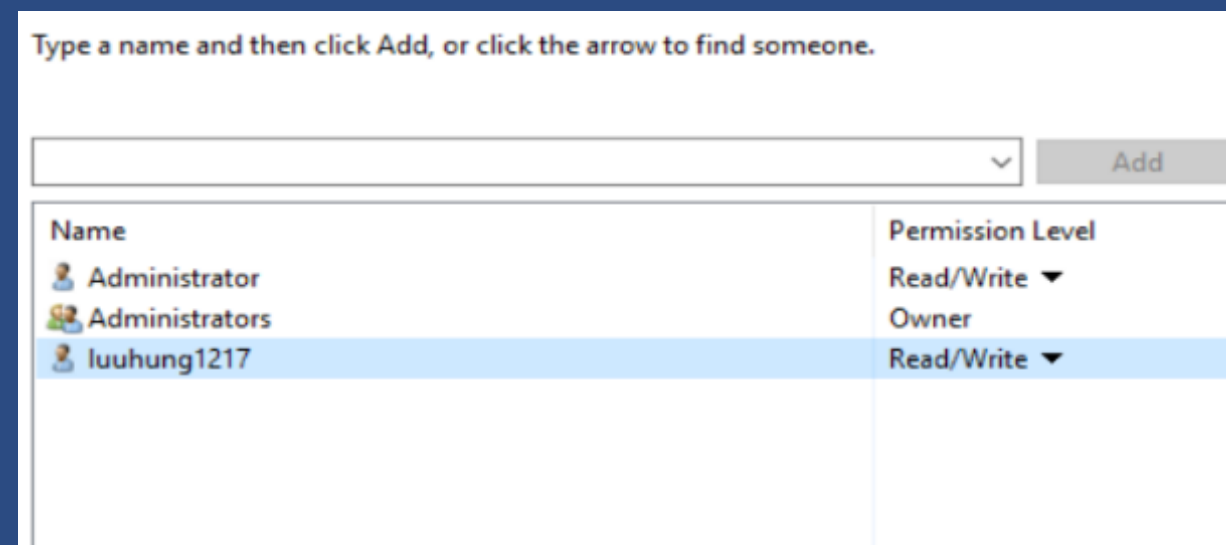
# Tạo user luuhung1217 và phân quyền truy cập các file cho user đó

## WINDOWS

Tạo user có tên luuhung1217 trong domain



Tạo file winlinux.txt và phân quyền đọc ghi cho user này



## LINUX

Tạo user có tên luuhung1217

```
luuvanhung@luuvanhung-virtual-machine: ~  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
luuvanhung@luuvanhung-virtual-machine:~$ sudo useradd -m luuhung1217  
[sudo] password for luuvanhung:  
luuvanhung@luuvanhung-virtual-machine:~$ sudo useradd -m luuhung1217  
useradd: user 'luuhung1217' already exists  
luuvanhung@luuvanhung-virtual-machine:~$ sudo passwd luuhung1217  
New password:  
Retype new password:  
Sorry, passwords do not match.  
New password:  
Retype new password:  
passwd: password updated successfully  
luuvanhung@luuvanhung-virtual-machine:~$
```

Tạo file winlinux.txt và phân quyền đọc ghi cho file này

```
luuvanhung@luuvanhung-virtual-machine:~/Desktop$ touch winlinux.txt  
luuvanhung@luuvanhung-virtual-machine:~/Desktop$ sudo chown luuhung1217 winlinux.txt  
luuvanhung@luuvanhung-virtual-machine:~/Desktop$ sudo chmod 744 winlinux.txt
```





## DỊCH VỤ TRUY NHẬP TỪ XA

Dịch vụ truy nhập từ xa cho phép người dùng kết nối từ bên ngoài vào máy chủ dịch vụ bên trong, để truy nhập dữ liệu và các ứng dụng như làm việc trên máy tính thông thường





# WINDOWS

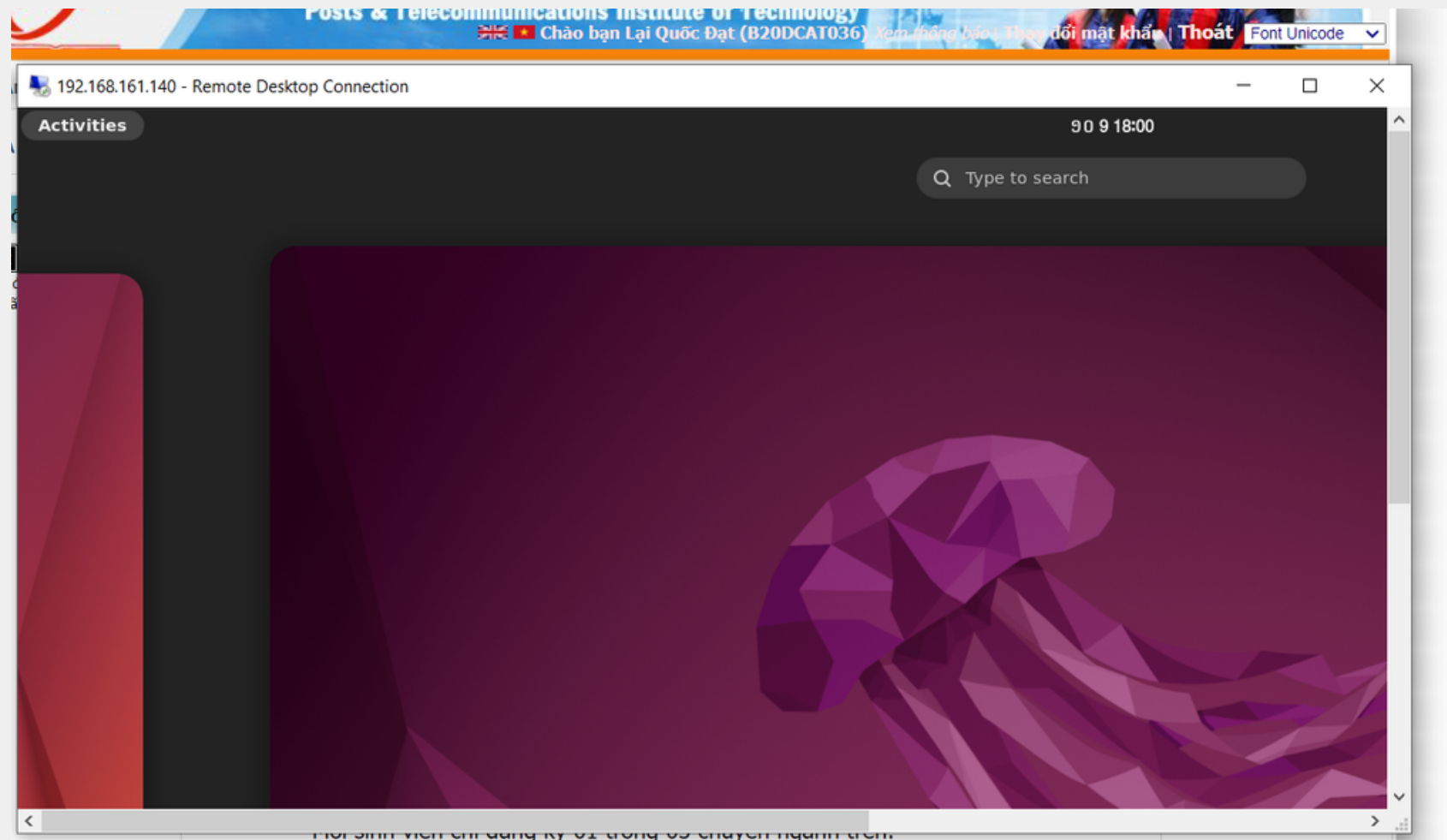
- Nguy cơ mất dữ liệu cao, có khả năng bị sập nếu quá tải người truy cập
- Cài đặt và quản trị phức tạp
- Sử dụng kết nối để trao đổi sử dụng dữ liệu
- Cần đăng nhập user và pass mỗi khi kết nối.
- Tiêu tốn nhiều tài nguyên
- Các công cụ hỗ trợ truy nhập từ xa: TeamViewer, UltraViewer, PuTTY,...

# LINUX

- Tính an toàn dữ liệu cao.
- Cài đặt và quản trị đơn giản.
- Sử dụng kết nối có thể sử dụng các câu lệnh điều khiển, trao đổi dữ liệu từ máy chủ đến máy trạm và ngược lại.
- Có thể sử dụng tạo key để xác thực không cần pass giúp bảo mật password của user
- Tiêu tốn ít tài nguyên.
- Các công cụ hỗ trợ truy nhập từ xa: OpenSSH, Puppet, Zentyal,...

# WINDOWS

- Cài đặt xrdp để có thể thực hiện truy nhập từ xa trên Ubuntu. Chạy lệnh `sudo systemctl enable xrdp` để khởi động dịch vụ
- Sử dụng Remote Desktop Connection có sẵn trên Windows.
- Nhập địa chỉ ip của máy Ubuntu sau đó nhấn connect



# LINUX

- Cài đặt trên máy chủ: `sudo apt-get install openssh-server`. Cài đặt trên máy khách: `sudo apt-get install openssh-client`.
- Tạo khóa công khai và bí mật để sử dụng trong dịch vụ SSH qua câu lệnh `ssh-keygen -t rsa`

```
(kali@B20DCAT135-Nhi-Kali)-[~]
$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/id_rsa
Your public key has been saved in /home/kali/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:rsuWM9L5oTlp+jAuwE7hPqBTblLZXzKW7AP2qtpntnQ kali@B20DCAT135-Nhi-Kali
The key's randomart image is:
+--[RSA 3072]--+
|
|o .o + .S
|o++ + B..
|*= +BEB0
|+=+0*+#+ .
|.+++BBB.
+--[SHA256]--+
```

- Để sử dụng khóa công khai, người dùng cần chép khóa vào máy chủ

```
& Telecommunications Institute of Technology
Chào bạn Lục Nguyễn Trang Nhi (B20DCAT135) Xem thông báo | Thay đổi mật khẩu | Thoát

root@ninhnohope: ~
root@ninhnohope:~# ssh kali@192.168.11.135
kali@192.168.11.135's password:
Linux B20DCAT135-Nhi-Kali 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.0-1kali6 (2022-07-07) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Oct 17 12:30:56 2022 from 192.168.11.132
(kali@B20DCAT135-Nhi-Kali)-[~]
$ exit
```

**GIÁM SÁT HOẠT ĐỘNG  
VÀ KIỂM TOÁN.  
TÌM HIỂU VÀ PHÂN  
TÍCH LOG**



# Giám sát (Monitoring)

Là quá trình theo dõi việc vận hành của hệ thống để xác lập tiêu chuẩn cơ sở, xác định và xử lý vấn đề tiềm năng.



## Windows

Gồm 4 công cụ giám sát:

- Giám sát hiệu năng
- Quản lý công việc
- Giám sát tài nguyên
- Xem bản ghi sự kiện

Hệ thống giám sát sử dụng giao diện đồ họa

File xuất ra có thể lưu dưới nhiều dạng như excel, vsc,...

## Linux

Gồm bộ công cụ:

- ps (có sẵn)
- df(có sẵn)
- netstat(cài đặt thêm)
- sysstat(cài đặt thêm)

Hệ thống giám sát sử dụng giao diện dòng lệnh.

File chỉ được xuất ra dưới dạng thuần text



# Kiểm toán (Auditing)

Kiểm toán giúp ta làm được những việc sau:

- Theo dõi truy nhập file và thay đổi
- Giám sát các lời gọi và chức năng hệ thống
- Phát hiện các bất thường như các tiến trình bị hỏng/ngưng.
- Các câu lệnh thực hiện bởi người dùng

## WINDOWS

Hệ điều hành Windows cung cấp một số công cụ kiểm toán như WinAudit và Local Security Policy.

Các chính sách tiêu biểu:

- Đăng nhập
- Quản lý tài khoản
- Theo dõi chi tiết
- Truy nhập thư mục động
- Truy nhập đối tượng



## LINUX

Sử dụng công cụ auditd được cài đặt qua câu lệnh: `apt-get install`.

Hệ thống kiểm toán Linux có một số ưu điểm:

- Cho phép xem bất kỳ hoạt động hệ thống nào
- Hỗ trợ phát hiện, phân tích các cam kết bảo mật tiềm năng của một hệ thống.
- Không phụ thuộc vào các yếu tố bên ngoài hệ điều hành.
- Lưu trữ tất cả việc sử dụng các cơ chế xác thực (SSH, Kerberos,...)

# So sánh dịch vụ kiểm toán

## Windows

- Hệ thống kiểm toán được tích hợp sẵn trên hệ điều hành.
- Sử dụng giao diện đồ họa dễ dàng quan sát và sử dụng.
- File xuất ra có thể lưu dưới nhiều định dạng: excel, vsc.

## Linux

- Hệ thống kiểm toán chưa được tích hợp sẵn trên hệ điều hành.
- Sử dụng giao diện dòng lệnh, khó khăn trong việc quan sát và sử dụng.
- File xuất ra dưới dạng thuần text.



# Tìm hiểu và phân tích các loại log

LOG LÀ MỘT PHẦN THÔNG TIN QUAN TRỌNG ĐƯỢC CUNG CẤP ĐỂ GHI LẠI CÁC SỰ KIỆN, HÀNH ĐỘNG DIỄN RA TRONG THỜI GIAN CHẠY DỊCH VỤ HAY ỨNG DỤNG.

## WINDOWS

- Trên Windows Log được lưu tại `C:\Windows\System32\winevt\Logs`
- Tương tác và tìm kiếm file log dễ dàng thông qua giao diện.
- Sử dụng các file evtx để lưu trữ, cần có phần mềm cụ thể thì mới có thể đọc.
- Quản lý theo nhóm ứng dụng, sau đó phân theo eventId

## LINUX

- Các tập tin được đặt trong thư mục `/var/log`
- Tương tác thông qua các command dẫn đến việc khó khăn trong tìm kiếm file log.
- Lưu dưới dạng text thuần túy, dễ dàng đọc.
- Quản lý dựa trên ứng dụng, mỗi ứng dụng có 1 file log riêng.

# Các loại log

## WINDOWS

- Application Log: Ghi lại những sự kiện xảy ra của ứng dụng.
- Security Log: Ghi lại các sự kiện dựa trên các quy chuẩn trong local hay global group policies.
- System Log: Các sự kiện được ghi lại bởi hệ điều hành.
- Setup: xác định các bản cập nhật bảo mật, bản vá của Windows.
- Forwarded Events: thu nhận các log được gửi từ các hệ thống khác về 1 hệ thống tạm gọi là hệ thống “thu nhập”.

## LINUX

Các file log được chia thành 4 loại:

- Application Logs: Nhật ký ứng dụng
- Event Logs: Nhật ký sự kiện
- Service Logs: Nhật ký dịch vụ
- System Logs: Nhật ký hệ thống