

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



BÁO CÁO BÀI TẬP LỚN
MÔN HỌC: HỆ ĐIỀU HÀNH WINDOWS
VÀ LINUX/UNIX

Giảng viên hướng dẫn: Đinh Trường Duy

Sinh viên thực hiện: Nhóm D20N03G03

Phạm Công Thuộc - B20DCAT187

Lục Nguyễn Trang Nhi - B20DCAT135

Trần Quốc Huy - B20DCAT086

Lại Quốc Đạt - B20DCAT036

Lưu Văn Hưng - B20DCAT088

Hà Nội, 10/2022

MỤC LỤC

I. CHIA SẺ FILE VÀ MÁY IN.....	3
1. Dịch vụ chia sẻ file và máy in.....	3
2. Cài đặt và quản trị file trên Windows và Linux:.....	4
3. Ưu, nhược điểm của Windows và Linux khi chia sẻ file và máy in:.....	4
II. QUẢN LÝ TRANG WEB	5
1. Giới thiệu về dịch vụ web	5
2. Quản lý trang web trên Windows và Linux	5
3. Ưu/nhược điểm của windows và linux với tư cách hệ điều hành máy chủ web.....	7
III. QUẢN LÝ NGƯỜI DÙNG VÀ MÁY TÍNH	8
1. Windows:	8
2. Linux(Ubuntu):	8
3. Quản lý người dùng trên hệ điều hành Windows và Linux:	9
4. So sánh quản lý người dùng và máy tính trong Windows và Linux.....	9
IV. DỊCH VỤ TRUY NHẬP TỪ XA	10
1. Windows	10
2. Linux	10
3. So sánh dịch vụ truy nhập từ xa giữa Windows và Linux	10
4. Kịch bản demo	11
V. GIÁM SÁT HOẠT ĐỘNG VÀ KIỂM TOÁN. TÌM HIỂU VÀ PHÂN TÍCH VỀ CÁC LOẠI LOG	12
1. Giám sát hoạt động và kiểm toán.....	12
2. Tìm hiểu và phân tích các loại log	13
3. Kịch bản phát hiện đăng nhập dựa theo log.....	15

NHẬT KÝ HOẠT ĐỘNG NHÓM

Thành viên	Công việc
Phạm Công Thuộc (nhóm trưởng)	Giám sát hoạt động và kiểm toán. Tìm hiểu và phân tích về các loại log
Lục Nguyễn Trang Nhi	Quản lý trang web
Trần Quốc Huy	Chia sẻ file và máy in
Lại Quốc Đạt	Dịch vụ truy nhập từ xa
Lưu Văn Hưng	Quản lý người dùng và máy tính

I. CHIA SẺ FILE VÀ MÁY IN

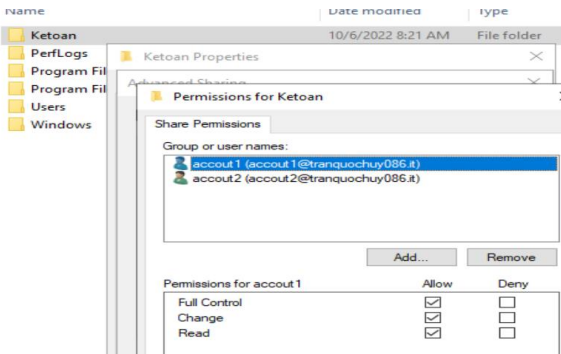
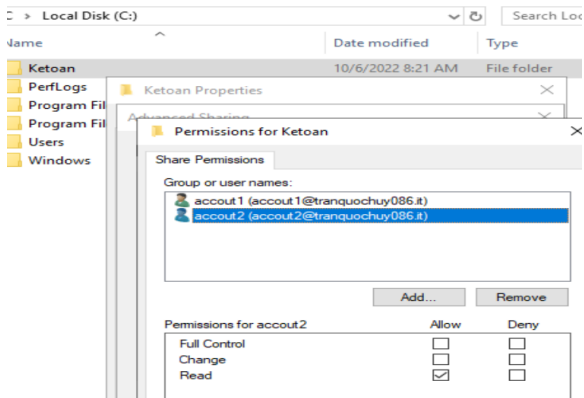
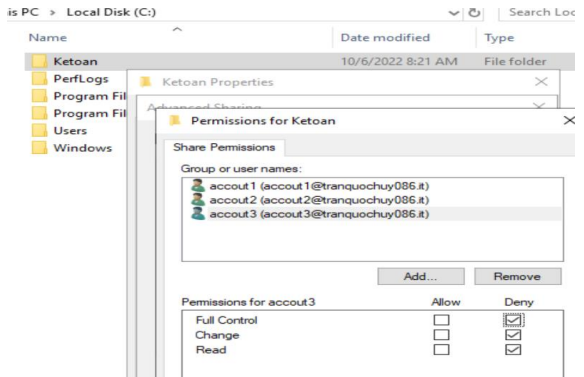
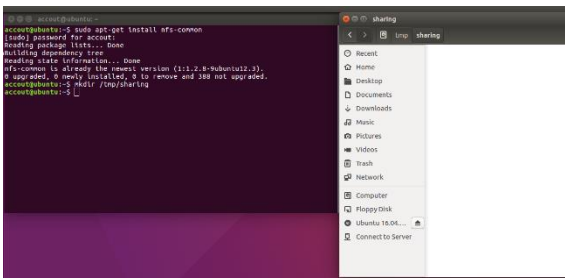
1. Dịch vụ chia sẻ file và máy in

	Windows	Linux
Chia sẻ file	<p>Việc truy nhập thành công các file chia sẻ phải căn cứ vào quyền truy nhập mà người dùng có được. Trong môi trường Windows có thể áp dụng hai hình thức đảm bảo an ninh:</p> <ul style="list-style-type: none"> - 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 - Đặt quyền file/thư mục sử dụng cách thức phân quyền NTFS để kiểm soát việc truy nhập. Hình thức này cho phép giám sát tốt hơn và các quyền chi tiết hơn. 	<p>Dịch vụ NFS (Network File System) là dịch vụ chia sẻ file trong môi trường Linux/Unix. Dịch vụ này cho phép người dùng sử dụng file/thư mục trên máy tính mạng giống như trong ổ đĩa cục bộ. Dịch vụ NFS hoạt động theo mô hình chủ/khách trong đó:</p> <ul style="list-style-type: none"> - Máy chủ chia sẻ thư mục /shared - Máy khách truy nhập vào thư mục chia sẻ trên máy chủ server:/shared qua câu lệnh mount - Ưu điểm của dịch vụ NFS là cho phép tiết kiệm không gian lưu trữ trên các máy trạm nhờ vào việc cất giữ các dữ liệu dùng chung lên máy chủ mà truy cập được qua mạng. Người dùng không cần phải có thư mục gốc (home) riêng biệt trên các máy trạm. <p>Giao thức truyền file FTP:</p> <ul style="list-style-type: none"> - Là giao thức cho phép tải các file giữa các máy tính nối mạng Internet. - Phương pháp này chỉ phù hợp để trao đổi các file dùng chung như các file phần mềm. - Để sử dụng dịch vụ này trên máy khách cần có chương trình ftp - Máy chủ FTP cung cấp hai chế độ kết nối: Nặc danh và Xác thực.
Chia sẻ máy in	<p>Các máy in mạng được kết nối trực tiếp với mạng hay thông qua máy tính. Các máy chủ in ấn là máy tính kết nối với máy in và làm nhiệm vụ xử lý các yêu cầu in ấn từ các người dùng trong mạng.</p> <ul style="list-style-type: none"> - Thiết bị in (máy in vật lý): kết nối trực tiếp với máy chủ - Máy in (máy in lô-gíc): giao tiếp với máy in vật lý - Trình điều khiển máy in: giúp giao tiếp với máy in và che dấu thông tin chi tiết về máy in. <p>Các truy nhập của người dùng tới máy in chia sẻ chịu kiểm soát quyền truy nhập.</p> <ul style="list-style-type: none"> - Quyền in: được phép gửi tài liệu tới máy in để in ra. - Quyền quản lý máy in: Cho phép người dùng thay đổi cài đặt và cấu hình máy in. - Quyền quản lý tài liệu in: Hủy, dừng, in lại hay khởi động lại máy in. 	<p>Dịch vụ CUPS (Common UNIX Printing System) cung cấp dịch vụ in ấn và quản lý in cho người dùng sử dụng giao thức chuẩn in ấn Internet (Internet Printing Protocol). Dịch vụ CUPS cũng hỗ trợ PPD (PostScript Printer Description), tự động phát hiện các máy in mạng và cung cấp các công cụ quản trị và đặt cấu hình đơn giản qua Web.</p> <ul style="list-style-type: none"> - Phía máy khách sử dụng câu lệnh lpr để in các file tài liệu cần thiết theo dạng : lpr file_cần_in. - Trong quá trình hoạt động, CUPS ghi nhật ký hoạt động vào thư mục /var/log/cups.

2. Cài đặt và quản trị file trên Windows và Linux:

Trên máy server tạo các user account1, account2, account3 với password là abc123*. Tạo folder *Ketoan* trong phân vùng C. Đăng nhập máy server với user Administrator và chia sẻ folder này.

Cấp quyền cho user account1 được toàn quyền truy cập trên folder *Ketoan*. User account2 chỉ được phép xem folder *Ketoan*. User account3 không được phép truy cập folder *Ketoan*.

	Windows	Linux
Cài đặt	<p>Quyền account1: Toàn quyền</p>  <p>Quyền account2: Chỉ đọc</p>  <p>Quyền account3: Không được phép truy cập</p> 	<ul style="list-style-type: none"> Cài đặt NFS trên Server: <pre>sudo apt-get install nfs-kernel-server</pre> mở tập tin /etc/exports: <pre>sudo nano /etc/exports</pre> chia sẻ thư mục này cho account1 với toàn quyền, account2 với quyền xem, account3 với không có quyền truy cập: <pre>/home/Ketoan 192.168.244.139(rw) account2(ro) account3(noaccess)</pre> Cài đặt NFS trên Client: <ul style="list-style-type: none"> cài gói nfs-common khi muốn truy cập vào Server mà không chia sẻ dữ liệu: <pre>sudo apt-get install nfs-common</pre> tạo 1 thư mục để mount thư mục Ketoan mà Server chia sẻ, tạo ở thư mục /tmp: <pre>mkdir /tmp/sharing</pre> tạo 1 thư mục để mount thư mục Ketoan mà Server chia sẻ, tạo ở thư mục /tmp: <pre>mkdir /tmp/sharing</pre>  <ul style="list-style-type: none"> Bây giờ mount thư mục Ketoan: <pre>sudo mount 192.168.254.133:/home/Ketoan /tmp/sharing</pre> Tương tự với account2 và account3 <p>Nếu mount thành công thì account có thể vào thư mục /tmp/sharing để truy cập các dữ liệu trong mục /home/Ketoan của Server.</p>

3. Ưu, nhược điểm của Windows và Linux khi chia sẻ file và máy in:

	Windows	Linux
Chia sẻ file	<p>Ưu điểm:</p> <ul style="list-style-type: none"> Đơn giản hóa việc chia sẻ và quản lý, dễ sử dụng 	<p>Ưu điểm:</p> <ul style="list-style-type: none"> FTP: <ul style="list-style-type: none"> Cho phép truyền nhiều tập tin cùng lúc

	<ul style="list-style-type: none"> - Hệ điều hành cung cấp tiện ích quản lý tài nguyên máy chủ file - Có thể khôi phục lại tính nhất quán của hệ thống tập tin tại thời điểm máy không may bị mất điện đột ngột hoặc hỏng hệ thống <p>Nhược điểm:</p> <ul style="list-style-type: none"> - Yêu cầu đủ tốc độ mạng - Giải quyết nhiều phân vùng cùng lúc và lãng phí không gian 	<ul style="list-style-type: none"> - Cho phép chuyển tệp tin nếu không may mất kết nối - Có khả năng đồng bộ hóa tập tin - Cho phép thêm dữ liệu vào khung chờ và lên lịch truyền - Tự động chuyển tập tin bằng script <p>▪ NFS:</p> <ul style="list-style-type: none"> - Tiết kiệm chi phí và không gian lưu trữ - Cho phép quản lý trung tâm <p>Nhược điểm:</p> <p>▪ FTP:</p> <ul style="list-style-type: none"> - Bảo mật kém - Để sử dụng thì máy khách cũng phải có chương trình FTP <p>▪ NFS:</p> <ul style="list-style-type: none"> - Không an toàn, chủ nên sử dụng trên 1 mạng đáng tin cậy sau Firewall - NFS bị chậm trong khi lưu lượng mạng lớn - Client và server tin tưởng lẫn nhau hoàn toàn
Chia sẻ máy in	<p>Ưu điểm:</p> <ul style="list-style-type: none"> - Cho phép nhiều người dùng chia sẻ cùng 1 máy in. Việc chia sẻ máy in được thực hiện dễ dàng thông qua giao diện windows - Dễ dàng quản lý hệ thống máy in và bản in <p>Nhược điểm:</p> <ul style="list-style-type: none"> - Khi gặp sự cố sẽ khó tìm được nguồn gốc nguyên nhân 	<p>Ưu điểm:</p> <ul style="list-style-type: none"> - CUPS cho phép tích hợp dễ dàng các tài nguyên in ấn cho cả hệ điều hành nguồn mở và độc quyền trong một mạng đồng nhất. - Một hệ thống in tiêu chuẩn, có thể xử lý nhiều định dạng dữ liệu trên máy chủ in. <p>Nhược điểm:</p> <ul style="list-style-type: none"> - Khó thao tác

II. QUẢN LÝ TRANG WEB

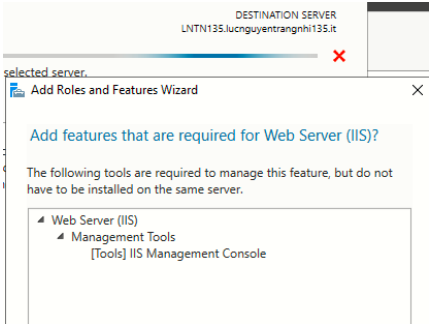
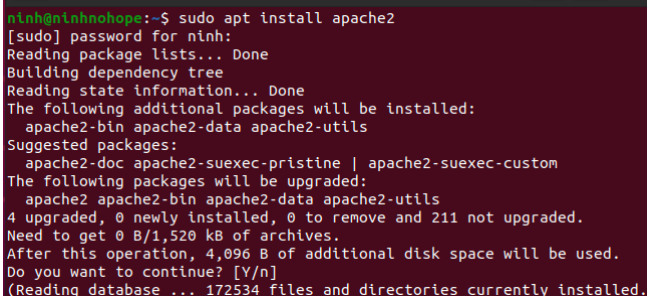
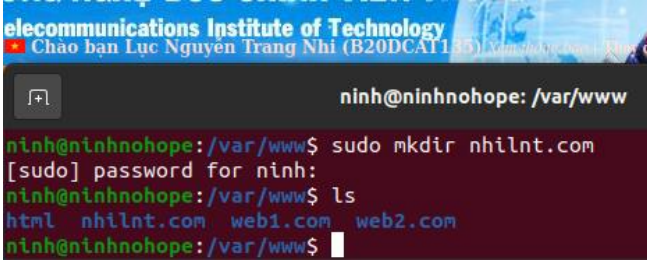
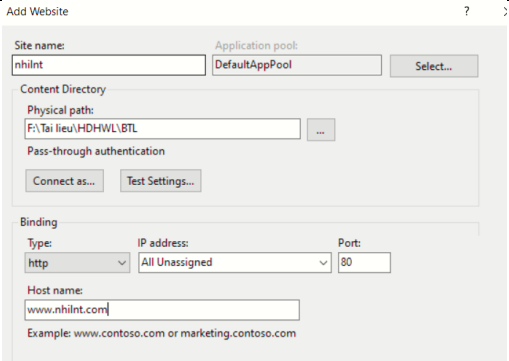

1. Giới thiệu về dịch vụ web

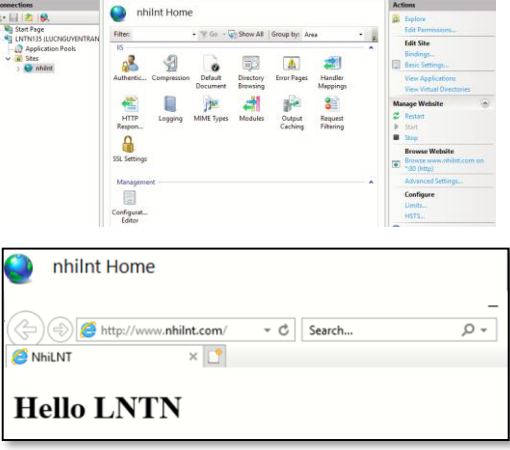
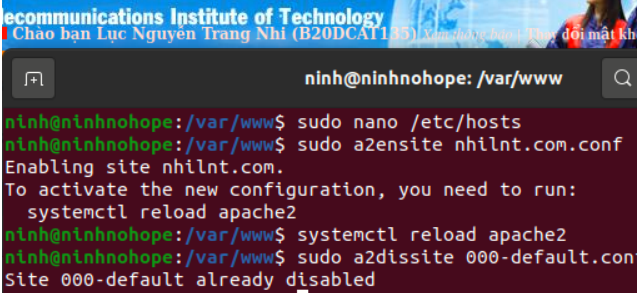
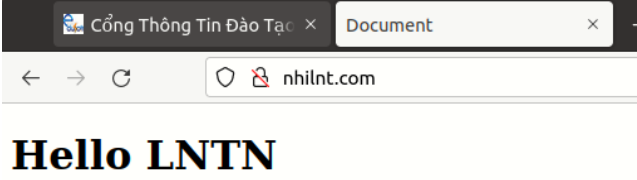
- Web là hệ thống các tài liệu dạng siêu văn bản liên kết với nhau (trang web) mà người dùng có thể xem được nhờ trình duyệt.
- Các trang web được lưu trong máy chủ web và dùng cổng số 80 để người dùng truy nhập vào.
- Đối với hệ điều hành Windows dịch vụ Web được cung cấp thông qua dịch vụ thông tin IIS (Internet Information Services). Ngược lại đối với hệ điều hành Linux được cung cấp thông tin qua máy chủ Web Apache.
- Máy chủ Web về cơ bản là phần mềm chịu trách nhiệm nhận các truy vấn dưới chuẩn giao thức truyền siêu văn bản từ máy khách, sau đó gửi trả kết quả xử lý thường dưới dạng các tài liệu theo chuẩn HTML.

2. Quản lý trang web trên Windows và Linux

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

	Windows	Linux/Unix
Khái niệm	- IIS – phần mềm mở rộng của Microsoft dùng để triển khai các dịch vụ web server	- Apache là một máy chủ Web sử dụng mã nguồn mở. Được triển khai ở nhiều nơi như Amazon, IBM. Máy chủ Apache đảm bảo:

	và xuất bản nội dung trang web lên Internet	<ul style="list-style-type: none"> • Ổn định và linh hoạt • An toàn và mềm dẻo.
Cách thức hoạt động	<ul style="list-style-type: none"> - IIS chỉ hoạt động trên Windows - Cách thức thực hiện dễ dàng, thuận tiện qua GUI của tiện ích quản lý IIS 	<ul style="list-style-type: none"> - Apache hoạt động trên nhiều hệ thống Linux/Unix và Windows - Sử dụng command line
Cài đặt	<p>Cài đặt IIS qua Server Manager</p> 	<p>Cài đặt Apache thông qua Terminal: Gõ lệnh <code>sudo apt-get install apache2</code></p> 
Cách tạo 1 trang web mới	<p>Sử dụng công cụ IIS, trong Connection:</p> <ul style="list-style-type: none"> - Chọn vị trí cây site - Đặt được dẫn vật lý lưu trữ các file - Đặt mật khẩu (nếu cần) xác định user - Xác định địa chỉ IP trang web 	<p>Tạo folder nhilnt.com là tên địa chỉ web mới trong file /var/www</p>  <p>Tạo địa chỉ mới dựa vào cấu hình ngầm định:</p> <pre>sudo cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/nhilnt.com.conf</pre> <ul style="list-style-type: none"> - Khởi tạo địa chỉ web mới: <pre>sudo a2ensite nhilnt.com.conf</pre> <pre>systemctl reload apache2</pre> <ul style="list-style-type: none"> - Tắt địa chỉ web: <pre>sudo a2dissite nhilnt.com.conf</pre> <pre>systemctl reload apache2</pre>
Cấu hình		<p>Tạo địa chỉ web mới dựa vào cấu hình ngầm định</p>  <p>Khởi tạo địa chỉ trang web mới và tắt địa chỉ Web mặc định trên Apache</p>

		 <p>Truy cập vào trang web</p> 
Xác thực trang web	<ul style="list-style-type: none"> - Nặc danh (Anonymous) - Xác thực cơ bản (Basic Authentication) - Xác thực số (Digest Authentication) - Xác thực Windows (Windows Authentication) 	<p>Apache cung cấp 2 khả năng xác thực người dùng là Basic authentication và Digest authentication.</p>

3. Ưu/nhược điểm của windows và linux với tư cách hệ điều hành máy chủ web

	Ưu điểm	Nhược điểm
Windows	<ul style="list-style-type: none"> • Hoạt động trực quan, thân thiện với user qua giao diện người dùng đồ họa • Trình điều khiển cho phần cứng được cập nhật nhanh chóng và dễ dàng • Cập nhật hệ thống tự động hóa dễ dàng và tùy chọn. Đảm bảo hỗ trợ lâu dài • Có thể giải quyết các vấn đề kỹ thuật thông qua việc khôi phục hệ thống • Hỗ trợ một số lượng lớn các ứng dụng của bên thứ ba • Tương thích với các chương trình độc quyền và phổ biến của Microsoft như Sharepoint hoặc Exchange 	<ul style="list-style-type: none"> • Chi phí cao hơn do phí cấp phép bắt buộc cho hệ điều hành. • Tính bảo mật ở mức trung bình, làm mất tính ổn định của máy chủ nếu gặp trục trặc. Có thể khiến máy chủ windows hoạt động chậm và thậm chí bị tấn công bởi phần mềm độc hại và vi rút. • Sử dụng nhiều tài nguyên (do GUI bắt buộc) • Không phù hợp như một hệ thống nhiều người dùng
Linux /Unix	<ul style="list-style-type: none"> • Miễn phí • Người quản trị hệ thống có quyền tự do và cơ hội để tùy chỉnh hệ thống. • Hỗ trợ công việc hợp tác mà không làm hỏng cốt lõi của chương trình • Đáng tin cậy hơn - hiếm khi gặp phải phần mềm độc hại, các mối đe dọa mạng hoặc các lỗi bảo mật khác. • Không yêu cầu nhiều về phần cứng và tiêu thụ ít tài nguyên hơn, hiệu suất cao hơn • Tích hợp chức năng từ xa để quản trị từ xa 	<ul style="list-style-type: none"> • Hoạt động thông qua dòng lệnh thay vì GUI, yêu cầu có kinh nghiệm. • Một số chương trình của bên thứ ba chỉ có thể được cài đặt bởi quản trị viên • Quá trình cập nhật đôi khi có thể rất phức tạp • Không phải tất cả các phiên bản đều được hỗ trợ lâu dài • Một số chương trình chuyên nghiệp không hoạt động với Linux

Mặc dù Windows có thể giúp thiết lập tất cả những thứ này dễ dàng hơn Linux nhưng Linux tạo ra một máy chủ web tốt hơn. **Linux ổn định hơn, bảo mật hơn và nhanh hơn và miễn phí**

Linux có hỗ trợ PHP và MySQL, cài đặt WordPress dễ dàng hơn trên máy chủ Linux. Ngoài ra, nó cung cấp khả năng truy cập dễ dàng hơn vào HTTP, Apache và các công cụ tạo trang khác, các môi trường JavaScript và NodeJS cũng như các ngôn ngữ lập trình Perl và Python. Tuy nhiên, nếu bạn định phát triển các trang web bằng cách sử dụng khung công tác của Microsoft, chẳng hạn như khung ASP hoặc .NET, thì việc sử dụng chúng trên Windows Server sẽ đơn giản hơn nhiều.

III. QUẢN LÝ NGƯỜI DÙNG VÀ MÁY TÍNH

1. Windows:

- Mỗi một người dùng cần có tài khoản người dùng riêng. Tài khoản được sử dụng khi người dùng truy nhập vào mạng hoặc cho phép người dùng đăng nhập vào máy hay miền thư mục động.
- Để thuận tiện cho việc quản trị, Windows tạo sẵn một số tài khoản như quản trị (Admin) và khách (Guest). Ngoài ra, các người dùng có vai trò và yêu cầu tương tự nhau có thể được xếp vào nhóm người dùng (User group). Điều này giúp cho việc quản trị được dễ dàng và thuận tiện. Nhóm người dùng phân biệt thành:
 - Nhóm miền cục bộ (Domain local group)
 - Nhóm toàn thể (Global group)
 - Nhóm vạn năng (Universal group)
- Với mỗi tài nguyên có kiểm soát truy nhập người dùng có thể thực hiện hay cấp các quyền tiêu biểu như sau:
 - Toàn quyền kiểm soát: quyền ghi đọc, sửa và thực thi, thay đổi thuộc tính và quyền, lấy quyền sở hữu các đối tượng tài nguyên.
 - Sửa: Cho phép đọc ghi sửa và thay đổi thuộc tính đối tượng tài nguyên.
 - Đọc: Hiển thị dữ liệu, thuộc tính, chủ sở hữu và quyền của các đối tượng tài nguyên.
 - Ghi: Ghi/thêm dữ liệu vào đối tượng tài nguyên, đọc hoặc thay đổi các thuộc tính tài nguyên

2. Linux(Ubuntu):

- Linux là hệ điều hành hỗ trợ nhiều người dùng.
- User trong Linux gồm user và super user (root) - là tài khoản có quyền cao nhất trong hệ thống
- Mỗi user và group thường có đặc điểm như sau :
 - + Tên tài khoản user, group và mã định danh (uid, gid) là duy nhất.
 - + Mỗi user có thể thuộc về nhiều group.
 - + Tài khoản super user có uid=gid=0.
 - + Khi tạo ra 1 user thì mặc định 1 group mang tên user được tạo ra.

Một số thao tác với user và group:

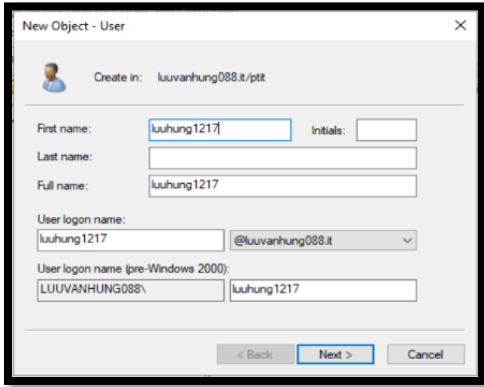
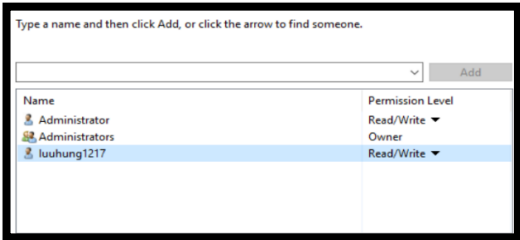
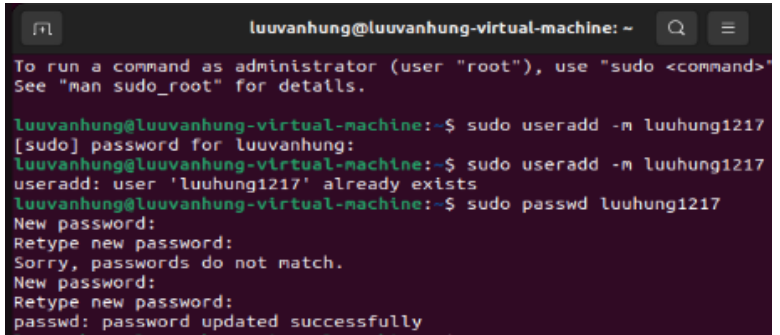
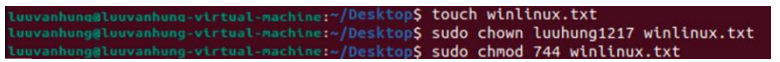
- + Thêm user mới: **# sudo useradd -m (tên user)**
- + Đặt mật khẩu cho user: **# sudo passwd (tên user)**
- + Thêm user vào một Group: **# sudo usermod -a -G (tên Group tên user)**
- + Xóa user khỏi 1 Group: **# sudo gpasswd -d (tên User, tên Group)**
- + Xóa user: **# sudo userdel (tên user)**
- + Thêm Group mới: **# sudo groupadd (tên Group)**
- + Xóa Group: **# sudo groupdel (tên Group)**
- + Thay đổi tên Group: **# sudo groupmod -n Newname Oldname**
- Người dùng có thể thay đổi quyền thông qua các câu lệnh sau chown và chmod.
 - chown cho phép 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

3. Quản lý người dùng trên hệ điều hành Windows và Linux:

Mục đích: Tạo user luuhung1217 và phân quyền truy cập các file cho user đó

Windows	Linux
<p>Tạo user có tên luuhung1217 trong domain</p>  <p>Tạo file winlinux.txt và phân quyền đọc ghi cho user này</p> 	<p>Tạo user có tên luuhung1217 bằng terminal</p>  <p>Tạo file winlinux.txt, chuyển owner của file sang user luuhung1217 và phân quyền đọc ghi, thực thi file cho user này</p> 

4. So sánh quản lý người dùng và máy tính trong Windows và Linux

		Windows	Linux (Ubuntu)
Tài khoản	Giống nhau	<ul style="list-style-type: none"> - Đều là HĐH nhiều người dùng nhưng có (Administrator hay Root) có quyền cao nhất - Đều có chức năng tạo, sửa, xóa User, phân quyền truy nhập - Mỗi User có tài khoản mật khẩu riêng biệt 	
	Khác nhau	<ul style="list-style-type: none"> - Windows có 4 loại user 📁 Đa dạng hơn về mặt người dùng - Có thể dùng Guest để đăng nhập nếu không có tài khoản - Thực hiện quản trị trên Computer Manager hay server Manager 	<ul style="list-style-type: none"> - Ubuntu có 2 loại user 📁 Bắt buộc phải có tài khoản nếu muốn sử dụng 📁 Không thể đăng nhập bừa bãi - Thực hiện quản trị bằng các dòng lệnh trên Terminal
Cách thêm bớt Users		<ul style="list-style-type: none"> - Ubuntu cho phép thêm bớt user bằng cả giao diện đồ họa và dòng lệnh 📁 Linux linh hoạt hơn ở mặt này 	
Quản trị group và file	Giống nhau	<ul style="list-style-type: none"> - Cả Windows và Ubuntu đều cho phép chia sẻ, đọc ghi file trong một group. - Cả hai đều cho phép phân quyền tài khoản theo ý muốn. 	
	Khác nhau	<ul style="list-style-type: none"> - Trong Windows, nếu muốn chia sẻ file thì phải join vào cùng một domain 	<ul style="list-style-type: none"> - Trong Ubuntu, có thể tạo group, user, phân quyền vô cùng nhanh chóng 📁 Ubuntu quản lý dễ dàng và nhanh chóng hơn so với Windows

IV. 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. Cùng với sự phát triển của các công nghệ truyền dữ liệu tốc độ cao dịch vụ truy nhập từ xa trở nên tiện dụng hơn.

1. Windows

Dịch vụ truy nhập từ xa thường sử dụng mạng riêng ảo VPN (*Virtual Private Networks*) hỗ trợ các giao thức:

- *Point-to-Point Tunneling Protocol (PPTP)*: Đơn giản khi triển khai song tính bảo mật yếu.
- *Layer 2 Tunneling Protocol (L2TP)*: Dùng chuẩn IPSec.
- *Secure Socket Tunneling Protocol (SSTP)*: dùng giao thức http bảo mật

Dịch vụ VPN được cung cấp thông qua dịch vụ truy nhập từ xa và định tuyến RRAS (Routing and Remote Access Services). Cũng giống như các dịch vụ máy chủ khác, dịch vụ RRAS được cài đặt thông qua “Server Manager”. Người quản trị có thể chọn chức năng VPN từ giao diện cài đặt RRAS.

Để sử dụng VPN, bên phía người dùng thực hiện việc cấu hình kết nối thông qua tiện ích quản trị kết nối mạng.

Ngoài việc sử dụng VPN để truy nhập vào các dịch vụ mà máy chủ cung cấp, người quản trị có thể sử dụng dịch vụ có kết quả tương tự đó là dịch vụ màn hình làm việc từ xa (Remote Desktop Connections). Dịch vụ này có số lượng kết nối rất hạn chế so với dịch vụ VPN.

Trong bản Server 2012, dịch vụ này có thể được thay thế bởi dịch vụ truy nhập trực tiếp (DirectAccess). Bên phía người dùng không cần thiết phải khởi tạo kết nối VPN để truy nhập vào các tài nguyên của miền. Để sử dụng dịch vụ này, máy tính của người dùng cần cài đặt bản Windows 7 Ultimate trở lên.

2. Linux

Telnet là công cụ truyền thống cho phép thực thi các câu lệnh trên máy chủ từ xa qua mạng trong môi trường Unix. Tuy nhiên, dữ liệu của telnet truyền dưới dạng văn bản không được mã hóa nên không đảm bảo an toàn cho người dùng.

OpenSSH là phiên bản miễn phí của dịch vụ truy nhập bảo mật SSH (Secure Shell) cung cấp công cụ hữu hiệu cho việc truy nhập máy chủ Linux/Unix qua mạng. SSH dựa trên cơ chế mã hóa khóa công khai để đảm bảo việc xác thực người dùng và trao đổi khóa bí mật giúp chống lại việc xâm phạm dữ liệu trao đổi trên đường truyền Internet.

OpenSSH bao gồm hai phần:

- Ứng dụng hoạt động trên máy chủ chờ yêu cầu kết nối từ người dùng
- Ứng dụng trên máy khách: gửi yêu cầu kết nối tới máy chủ

3. So sánh dịch vụ truy nhập từ xa giữa Windows và Linux

- Truy nhập từ xa giúp người sử dụng dễ dàng trong quá trình làm việc, truy nhập dữ liệu cơ quan tổ chức của mình...
- Người dùng có thể sử dụng tài nguyên chung không phụ thuộc vào vị trí địa lý, ít tốn thời gian và chi phí trong quá trình làm việc.
- Tốc độ truy nhập phụ thuộc vào tốc độ và trạng thái mạng Internet.

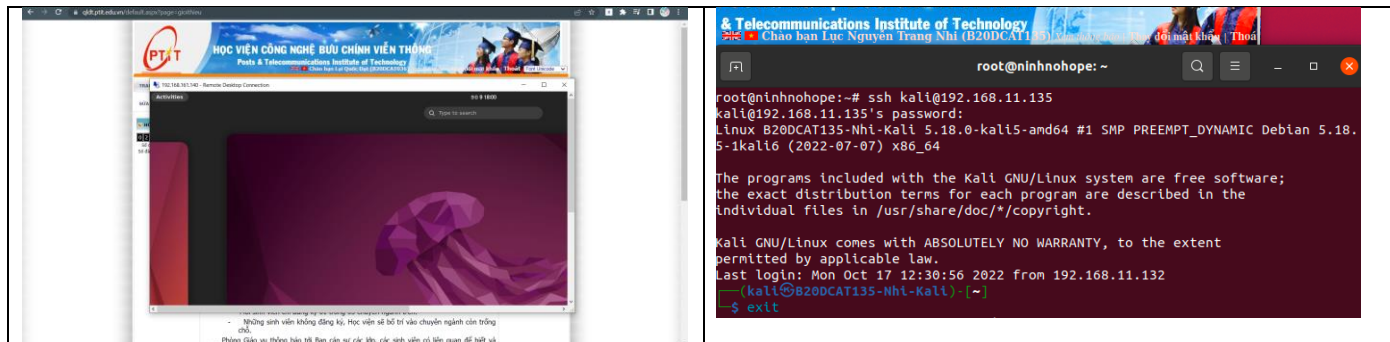
Windows	Linux
Nguy cơ mất dữ liệu cao, có khả năng sập nếu quá tải người truy nhập	Tính an toàn dữ liệu cao.
Truyền file chậm hơn so với Linux	Truyền file nhanh và an toàn hơn

Cung cấp cho người dùng giao diện đồ họa thông qua đó họ có thể truy cập vào máy tính từ xa và điều khiển nó 1 cách dễ dàng nhưng lại gây tiêu tốn nhiều tài nguyên	Sử dụng giao diện dòng lệnh, khó sử dụng đối với người mới. Tiêu tốn ít tài nguyên
Sử dụng kết nối để trao đổi dữ liệu. Sau khi khởi động, dịch vụ phía máy chủ RDP bắt đầu lắng nghe các yêu cầu kết nối trên cổng 3389.	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.
Cần đăng nhập user và pass mỗi khi kết nối	Máy khách SSH điều khiển quá trình thiết lập kết nối và sử dụng mã hóa khóa công khai để xác thực mà không cần dùng pass.

4. Kịch bản demo

Sử dụng các phần mềm truy nhập từ xa để truy nhập từ Windows vào Ubuntu và truy nhập từ Ubuntu vào Kali

Windows	Linux
<ul style="list-style-type: none"> Cài đặt xrdp để có thể thực hiện truy nhập từ xa trên Ubuntu  <ul style="list-style-type: none"> Chạy lệnh <code>sudo systemctl enable xrdp</code> để khởi động dịch vụ xrdp  <ul style="list-style-type: none"> Sử dụng Remote Desktop Connection. Remote Desktop App được tích hợp sẵn trong Windows, vì vậy bạn chỉ cần vào Start và gõ đoạn text <i>Remote Desktop Connection</i> là có thể mở được. Nhập địa chỉ ip của máy Ubuntu sau đó nhấn connect  <ul style="list-style-type: none"> Màn hình ubuntu được điều khiển bởi máy windows 	<ul style="list-style-type: none"> Cài đặt trên máy chủ: <code>sudo apt-get install openssh-server</code>.  <ul style="list-style-type: none"> Cài đặt trên máy khách: <code>sudo apt-get install openssh-client</code>. Thông tin cấu hình được lưu trong file <code>/etc/ssh/sshd_config</code>. Tạo khóa công khai và bí mật để sử dụng trong dịch vụ SSH qua câu lệnh <code>ssh-keygen -t rsa</code>  <ul style="list-style-type: none"> Khóa sinh ra gồm khóa công khai và bí mật và được lưu trong thư mục của người dùng. Để sử dụng khóa công khai trong quá trình xác thực, người dùng cần chép khóa vào máy chủ 



V. GIÁM SÁT HOẠT ĐỘNG VÀ KIỂM TOÁN. TÌM HIỂU VÀ PHÂN TÍCH VỀ CÁC LOẠI LOG

1. Giám sát hoạt động và kiểm toán

Hệ thống công nghệ thông tin là hệ thống vô cùng quan trọng. Với mức độ phát triển công nghệ hiện nay, thì việc đảm bảo an ninh cho hệ thống thông tin là một vấn đề cấp thiết. Chính vì thế, các hệ điều hành đã cung cấp một giải pháp hoàn chỉnh, đầy đủ cho phép mọi người dùng và các tổ chức thực hiện việc giám sát và kiểm toán cho các sự kiện cho một hệ thống.

Cả hai hệ điều hành Windows và Linux đều có những công cụ hỗ trợ giám sát và kiểm toán đi kèm.

1.1. Giám sát (Monitoring)

Cả 2 hệ điều hành đều có các công cụ hỗ trợ giúp giám sát chủ yếu về các yếu tố đi kèm với các thông tin thời gian, địa chỉ chi tiết:

- Tình trạng hệ thống, bộ nhớ, các ứng dụng đang chạy.
- Tình trạng kết nối mạng.
- Các thiết bị có liên kết với hệ thống
- Thông tin người dùng đăng nhập
- Lịch sử dữ liệu của các file

a. Hệ điều hành Windows

Cung cấp các công cụ giám sát:

- Performance Monitor: giám sát hiệu năng
- Event Viewer: bản ghi sự kiện
- Resource Monitor: giám sát tài nguyên
- Task Manager: quản lý công việc

b. Hệ điều hành Linux

Cung cấp các công cụ:

- ps (có sẵn): Thông báo về tài nguyên đang được sử dụng
- df (có sẵn): Thông báo về tình trạng lưu trữ hệ thống
- netstat (cài đặt thêm): theo dõi các kết nối mạng vào ra trên hệ thống.
- sysstat (cài đặt thêm): giám sát về các hoạt động hệ thống, các thiết bị kết nối với máy chủ, thao tác với file dữ liệu đi kèm với đó là các thông tin về thời gian.

1.2. 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

a. Hệ điều hành Windows

Hệ điều hành Windows cung cấp một số công cụ kiểm toán như WinAudit và Local Security Policy. Sau đây là phần giới thiệu công cụ kiểm toán WinAudit.

Để sử dụng, ta tiến hành đưa phần mềm lên hệ thống cần kiểm toán, sau đó chọn Run as Administrator.



WinAudit cung cấp nhiều mục khác nhau để tiến hành kiểm toán, nhằm có những đánh giá chính xác nhất khi thiết kế hệ thống:

- Cập nhật bản vá: Các bản vá giúp sửa các lỗi phát sinh.
- Đánh giá chính sách: Có thể kiểm tra cũng như thay đổi các chính sách về user, lịch sửa chữa, mật khẩu.
- Cấu hình máy chủ: kiểm tra Window Update.
- Cấu hình an ninh máy chủ: Sử dụng công cụ quét lỗ hổng Nessus để rà soát.
- Hệ thống chống mã độc: sử dụng anti-virus và tường lửa để phòng chống tấn công.
- Chính sách triển khai: Kiểm tra phần mềm máy chủ có phù hợp với chính sách.

b. Hệ điều hành Linux:

Linux cung cấp cho ta công cụ để kiểm toán an ninh hệ thống thông qua Linux Audit Daemon. Ta có thể xem tại địa chỉ mặc định `/var/log/audit/audit.log`.

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.
- Không phụ thuộc vào các yếu tố bên ngoài hệ điều hành.
- Lưu trữ tất cả các việc sử dụng cơ chế xác thực (SSH, ...)

Ngoài ra còn có thể sử dụng các công cụ như Splunk, NAGIOS để gia tăng hiệu quả kiểm toán

So sánh hoạt động giám sát và kiểm toán trên Windows và Linux

	Windows	Linux
Giám sát	Các hệ thống giám sát được tích hợp sẵn trên hệ điều hành, không cần phải cài đặt thêm.	Hệ thống giám sát chưa đầy đủ, cần phải cài đặt thêm netstat và sysstat. <i>netstat và sysstat có thêm nhiều thao tác giám sát cụ thể hơn so với Windows</i>
Kiểm toán	Hệ thống kiểm toán được tích hợp sẵn trên hệ điều hành nhưng chưa đầy đủ, cần phải cài đặt thêm	Hệ thống kiểm toán cần chưa tích hợp sẵn cần phải cài đặt thêm
Giao diện	Sử dụng giao diện đồ họa giúp dễ dàng quan sát và sử dụng.	Sử dụng giao diện dòng lệnh nên người chưa có kinh nghiệm sẽ gặp khó khăn trong việc quan sát và sử dụng.
Đầu ra	File xuất ra có thể lưu dưới nhiều định dạng như excel, vsc.	File xuất ra dưới dạng thuần text. Nên xem xét việc sử dụng các công cụ khác để giám sát.

2. 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 service hay ứng dụng. Tất cả thông tin trong file log giúp ích cho việc theo dõi hiệu suất, khắc phục sự cố và gỡ lỗi ứng dụng hay forensic.

2.1. Hệ điều hành Windows

Event Log của Windows được lưu trữ mặc định tại đường dẫn: “%SystemRoot%\System32\winevt\logs”. Người dùng có thể truy cập trực tiếp đường dẫn hoặc xem qua Event Viewer. Mặc định lượng log được lưu trong event log này không được nhiều

Các loại Log:

- *Application Log*: Ghi lại những sự kiện xảy ra của ứng dụng. Ví dụ: Lỗi khi khởi động ứng dụng.
- *Security Log*: Ghi lại các sự kiện dựa trên các quy chuẩn trong local hay global group policies. Ví dụ: ghi lại thông tin về kiểm soát truy cập chẳng hạn như các lần login fail, folder access.
- *System Log*: Các sự kiện được ghi lại bởi hệ điều hành. Ví dụ: lỗi dịch vụ không thể khởi động trong quá trình khởi động hệ thống.
- *Setup*: xác định các bản cập nhật bảo mật của Windows, các bản vá đã thêm vào hệ thống.
- *Forwarded Events*: đây là quan trọng nhất, thu nhận các log được gửi từ các hệ thống khác về 1 hệ thống tạm gọi là hệ thống “thu nhập”. Windows Audit Collection Service chịu trách nhiệm thu thập và chuyển tiếp log.

Cấu trúc của log có các trường sau:

#	Tên	Diễn Giải
1	Log Name	Tên của log mà sự kiện được lưu trữ, ví dụ như loại log liên quan Security thì nó là Security, nếu log liên quan ứng dụng thì nó là Application.
2	Source	Là hệ thống/ứng dụng sinh ra log, ví dụ sinh ra bởi McAfee thì nó là "McAfee".
3	Event ID	Là mã được gán cho mỗi loại sự kiện (anh em nên để ý cái này quan trọng sẽ làm việc nhiều sau này).
4	Level	Mức độ của sự kiện, có mấy loại như Information, Error, Warning,...
5	User	Là user thực thi liên quan đến sự kiện đang ghi nhận.
6	Logged	Thời gian khi sự kiện được sinh ra.
7	Task Category	Là loại danh mục được gán khi log sinh ra, ví dụ: Logon, Audit Policy Change,...
8	Keywords	Được gán bởi nguồn tạo nên sự kiện, ví dụ: Classic, Audit Success,...
9	Computer	Tên máy tính.
10	Description	Mô tả chi tiết.

Một số loại event trong log:

- Event liên quan đến quản lý tài khoản: là các event lưu lại khi tài khoản được tạo, chỉnh sửa.
- Event đăng nhập, đăng xuất tài khoản
- Event truy cập share folder/object
- Event về quản lý chính sách: sinh ra khi các thay đổi policy trên máy tính.
- Event về các dịch vụ trên windows: sinh ra khi liên quan các dịch vụ chạy trên windows.
- Event về LAN, Wireless: sinh ra khi liên quan đến các kết nối mạng.
- Event về tiến trình
- Event về thực thi chương trình: một số event thường gặp khi điều tra về các tiến trình lạ được thực thi liên quan đến các action của Windows Defender

2.2. Hệ điều hành Linux

Hệ điều hành Linux cung cấp một kho lưu trữ các file log trong thư mục /var/log.

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

Các file log quan trọng:

- *File log /var/log/syslog*: Chứa nhật ký hoạt động hệ thống. Đây là file log đầu tiên sẽ được kiểm tra nếu có sự cố trên hệ thống.

- File log `/var/log/auth.log`: chứa thông tin các truy nhập trên hệ thống trong máy chủ. File này giúp chúng ta quan sát đc các lần đăng nhập thất bại và điều tra các cuộc tấn công.
- File log `/var/log/kern.log`: đây là file vô cùng quan trọng chứa các thông tin ghi bởi kernel. Thông qua file này giúp chúng ta khắc phục các lỗi liên quan đến kernel.
- File log `/var/log/faillog`: chứa các thông tin người dùng đăng nhập thất bại. Đây là file giúp chúng ta có thể tìm ra bất kỳ vi phạm bảo mật liên quan đến username hoặc password.

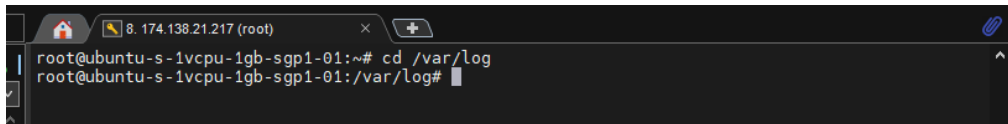
Ngoài các file log quan trọng cần kiểm tra đầu tiên khi hệ thống bị lỗi hoặc một vấn đề nào đó chúng ta còn có các file log khác chứa các thông tin khác nhau của hệ thống:

- `/var/log/daemon.log`: Chứa thông tin được ghi lại bởi các tiến trình chạy trên hệ thống.
- `/var/log/dpkg.log`: Chứa thông tin được ghi lại khi gói được cài đặt hoặc gỡ bỏ bằng lệnh `dpkg`.
- `/var/log/lastlog`: Hiện thị thông tin đăng nhập gần đây cho tất cả người dùng.
- `/var/log/alternigin.log`: Thông tin của các lựa chọn thay thế cập nhật được đăng nhập vào tệp nhật ký này.
- `/var/log/btmp`: Tập tin này chứa thông tin về các thông tin đăng nhập thất bại.
- `/var/log/wtmp`: Chứa các bản ghi đăng nhập. Sử dụng `wtmp` bạn có thể tìm ra ai đã đăng nhập vào hệ thống. Sử dụng `last` để xem thông tin file `wtmp`

3. Kịch bản phát hiện đăng nhập dựa theo log

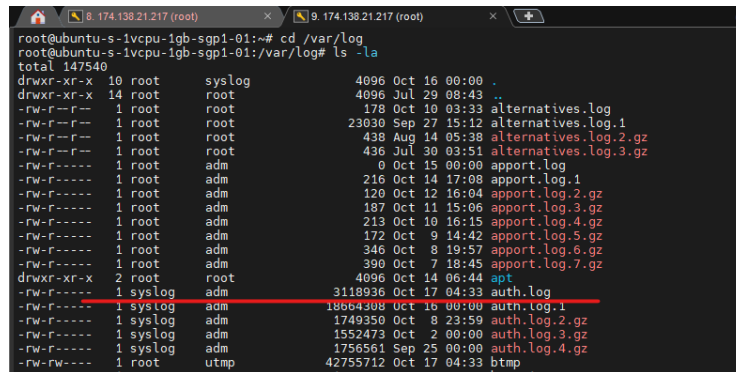
Mỗi khi đăng nhập vào windows hoặc user, hệ thống sẽ lưu lại các hành động xác thực bao gồm cả xác thực thành công hay thất bại.

Để có một ví dụ trực quan và đa dạng nhất, chúng ta sẽ tiến hành khảo sát trên một VPS (Virtual Private Server) chạy hệ điều hành Linux được public IP. Tiến hành truy cập đường đường dẫn: “`var/log`”.



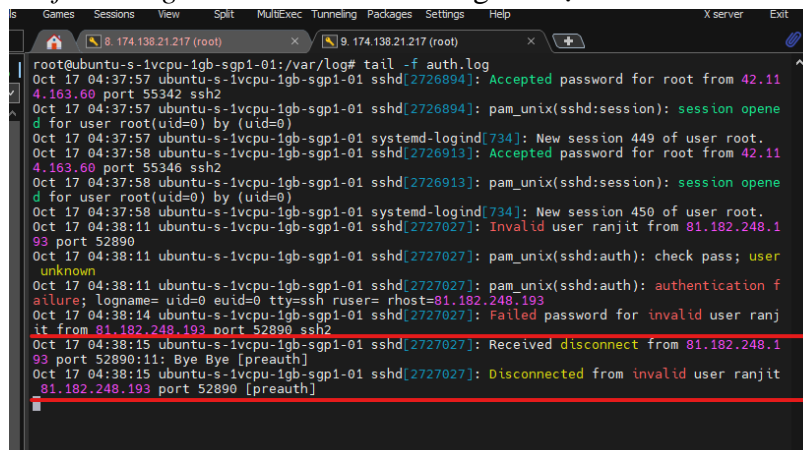
```
root@ubuntu-s-1vcpu-1gb-sgp1-01:~# cd /var/log
root@ubuntu-s-1vcpu-1gb-sgp1-01:/var/log#
```

Sử dụng lệnh “`ls -la`” để xem các file log liên quan. Và tiến hành khảo sát file `auth.log`



```
total 147540
drwxr-xr-x 10 root    syslog      4096 Oct 16 00:00 .
drwxr-xr-x 14 root    root         4096 Jul 29 08:43 ..
-rw-r--r-- 1 root    root         178 Oct 19 03:33 alternatives.log
-rw-r--r-- 1 root    root        23030 Sep 27 15:12 alternatives.log.1
-rw-r--r-- 1 root    root        438 Aug 14 05:38 alternatives.log.2.gz
-rw-r--r-- 1 root    root        436 Jul 30 03:51 alternatives.log.3.gz
-rw-r--r-- 1 root    adm          0 Oct 15 00:00 apport.log
-rw-r--r-- 1 root    adm        216 Oct 14 17:08 apport.log.1
-rw-r--r-- 1 root    adm       120 Oct 12 16:04 apport.log.2.gz
-rw-r--r-- 1 root    adm       187 Oct 11 15:06 apport.log.3.gz
-rw-r--r-- 1 root    adm       213 Oct 10 16:15 apport.log.4.gz
-rw-r--r-- 1 root    adm       172 Oct  9 14:42 apport.log.5.gz
-rw-r--r-- 1 root    adm       346 Oct  8 19:57 apport.log.6.gz
-rw-r--r-- 1 root    adm       390 Oct  7 18:45 apport.log.7.gz
drwxr-xr-x  2 root    root         4096 Oct 14 06:44 apt
-rw-r--r-- 1 syslog  adm     3118936 Oct 17 04:33 auth.log
-rw-r--r-- 1 syslog  adm    18664308 Oct 16 00:00 auth.log.1
-rw-r--r-- 1 syslog  adm    1749350 Oct  8 23:59 auth.log.2.gz
-rw-r--r-- 1 syslog  adm    1552473 Oct  2 00:00 auth.log.3.gz
-rw-r--r-- 1 syslog  adm    1758561 Sep 25 00:00 auth.log.4.gz
-rw-r--r-- 1 root    utmp     42755712 Oct 17 04:33 btmp
```

Sử dụng lệnh “`tail -f auth.log`” để theo dõi theo thời gian thực:



```
Oct 17 04:37:57 ubuntu-s-1vcpu-1gb-sgp1-01 sshd[2726894]: Accepted password for root from 42.114.163.60 port 55342 ssh2
Oct 17 04:37:57 ubuntu-s-1vcpu-1gb-sgp1-01 sshd[2726894]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Oct 17 04:37:57 ubuntu-s-1vcpu-1gb-sgp1-01 systemd-logind[734]: New session 449 of user root.
Oct 17 04:37:58 ubuntu-s-1vcpu-1gb-sgp1-01 sshd[2726913]: Accepted password for root from 42.114.163.60 port 55346 ssh2
Oct 17 04:37:58 ubuntu-s-1vcpu-1gb-sgp1-01 sshd[2726913]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Oct 17 04:37:58 ubuntu-s-1vcpu-1gb-sgp1-01 systemd-logind[734]: New session 450 of user root.
Oct 17 04:38:11 ubuntu-s-1vcpu-1gb-sgp1-01 sshd[2727027]: Invalid user ranjit from 81.182.248.193 port 52890
Oct 17 04:38:11 ubuntu-s-1vcpu-1gb-sgp1-01 sshd[2727027]: pam_unix(sshd:auth): check pass; user unknown
Oct 17 04:38:11 ubuntu-s-1vcpu-1gb-sgp1-01 sshd[2727027]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= root=81.182.248.193
Oct 17 04:38:14 ubuntu-s-1vcpu-1gb-sgp1-01 sshd[2727027]: Failed password for invalid user ranjit from 81.182.248.193 port 52890 ssh2
Oct 17 04:38:15 ubuntu-s-1vcpu-1gb-sgp1-01 sshd[2727027]: Received disconnect from 81.182.248.193 port 52890:11: Bye Bye [preauth]
Oct 17 04:38:15 ubuntu-s-1vcpu-1gb-sgp1-01 sshd[2727027]: Disconnected from invalid user ranjit 81.182.248.193 port 52890 [preauth]
```


Nhận xét: Người dùng có thể nhìn thấy một cách trực quan nhất về những lần đăng nhập thất bại (Failed password) hay ngắt kết nối (Disconnected) theo thời gian thực

Ngoài ra chúng ta tiến hành khảo sát thêm người dùng nào đang đăng nhập vào VPS:

```

root@ubuntu-s-1vcpu-1gb-sgp1-01: /var/log# lastlog
Username      Port      From      Last Log
root          pts/0    42.114.163.60  Mon Oct 17 04:43:14 +0000 2022
daemon                **Never logged in**
bin                  **Never logged in**
sys                  **Never logged in**
sync                 **Never logged in**
games                **Never logged in**
man                  **Never logged in**
lp                   **Never logged in**
mail                 **Never logged in**
news                 **Never logged in**
uucp                 **Never logged in**
proxy                **Never logged in**
www-data             **Never logged in**
backup               **Never logged in**
list                 **Never logged in**
irc                  **Never logged in**
gnats                **Never logged in**
nobody               **Never logged in**
systemd-network      **Never logged in**
systemd-resolve       **Never logged in**
messagebus            **Never logged in**
systemd-timesync      **Never logged in**
syslog                **Never logged in**
_apt                  **Never logged in**
tss                   **Never logged in**
uuid                  **Never logged in**
tcpdump              **Never logged in**
sshd                  **Never logged in**
pollinate             **Never logged in**
landscape             **Never logged in**
lxd                   **Never logged in**
dnsmasq               **Never logged in**
mysql                 **Never logged in**

```

Còn ở windows, có thể truy cập event viewer để kiểm tra

Security					Number of events: 32,901	
Keywords	Date and Time	Source	Event ID	Task Category		
Audit Success	10/19/2022 05:18:17 PM	Microsoft Windows security au...	5379	User Account Management		
Audit Success	10/19/2022 05:18:16 PM	Microsoft Windows security au...	5379	User Account Management		
Audit Success	10/19/2022 05:18:16 PM	Microsoft Windows security au...	5379	User Account Management		
Audit Success	10/19/2022 05:18:16 PM	Microsoft Windows security au...	5379	User Account Management		
Audit Success	10/19/2022 05:17:16 PM	Microsoft Windows security au...	5379	User Account Management		
Audit Success	10/19/2022 05:17:16 PM	Microsoft Windows security au...	5379	User Account Management		
Audit Success	10/19/2022 05:17:16 PM	Microsoft Windows security au...	5379	User Account Management		
Audit Success	10/19/2022 05:17:16 PM	Microsoft Windows security au...	5379	User Account Management		
Audit Success	10/19/2022 05:17:11 PM	Microsoft Windows security au...	5379	User Account Management		
Audit Success	10/19/2022 05:17:11 PM	Microsoft Windows security au...	5379	User Account Management		
Audit Success	10/19/2022 05:17:11 PM	Microsoft Windows security au...	5379	User Account Management		
Audit Success	10/19/2022 05:17:06 PM	Microsoft Windows security au...	5379	User Account Management		
Audit Success	10/19/2022 05:17:06 PM	Microsoft Windows security au...	5379	User Account Management		
Audit Success	10/19/2022 05:17:06 PM	Microsoft Windows security au...	5379	User Account Management		
Audit Success	10/19/2022 05:17:06 PM	Microsoft Windows security au...	5379	User Account Management		
Audit Success	10/19/2022 05:17:01 PM	Microsoft Windows security au...	5379	User Account Management		
Audit Success	10/19/2022 05:17:01 PM	Microsoft Windows security au...	5379	User Account Management		
Audit Success	10/19/2022 05:17:01 PM	Microsoft Windows security au...	5379	User Account Management		
Audit Success	10/19/2022 05:17:01 PM	Microsoft Windows security au...	5379	User Account Management		
Audit Success	10/19/2022 05:16:57 PM	Microsoft Windows security au...	5379	User Account Management		
Event 5379, Microsoft Windows security auditing.						
General Details						
Credential Manager credentials were read.						
Subject:						
Log Name:	Security	Source:	Microsoft Windows security	Logged:	10/19/2022 05:18:17 PM	
Event ID:	5379	Task Category:	User Account Management			
Level:	Information	Keywords:	Audit Success			
User:	N/A	Computer:	MSI			
OpCode:	Info					