BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỞNG ĐH SƯ PHẠM KỸ THUẬT TPHCM

KHOA ĐÀO TẠO CHẤT LƯỢNG CAO



ĐỀ TÀI: TRIỂN KHAI CÁC DỊCH VỤ MẠNG

TRÊN WINDOW/LINUX

Giảng viên hướng dẫn: Nguyễn Thị Thanh Vân

Sinh viên thực hiện:

Trần Quốc Việt 18110238

Trần Duy Đức Độ 18110098

TP.HCM, tháng 6 năm 2020

LỜI NHẬN XÉT

Điểm:

Nhận xét của giáo viên hướng dẫn:

Giáo viên hướng dẫn

Nguyễn Thị Thanh Vân

Mục Lục

[TÓM TẮT 4](#_Toc43196976)

[NỘI DUNG 5](#_Toc43196977)

[I. Giới thiệu tổng quan 5](#_Toc43196978)

[1. Bảng IP 5](#_Toc43196979)

[2. Mô hình OU. 5](#_Toc43196980)

[3. Kịch bản hoạt động. 5](#_Toc43196981)

[II. Mô tả chi tiết. 6](#_Toc43196982)

[1. Dịch vụ DHCP. 6](#_Toc43196983)

[2. Dịch vụ DNS và webservice. 6](#_Toc43196984)

[III. Mô phỏng tấn công mạng 8](#_Toc43196985)

[KẾT LUẬN 10](#_Toc43196986)

[I. Ưu điểm. 10](#_Toc43196987)

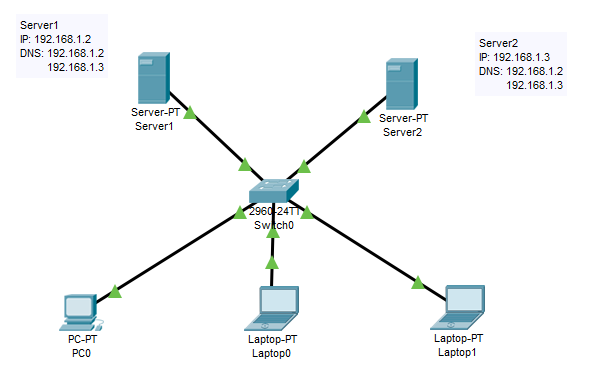
[II. Nhược điểm. 10](#_Toc43196988)

[III. Đề xuất cải tiến. 10](#_Toc43196989)

[TÀI LIỆU THAM KHẢO 11](#_Toc43196990)

# TÓM TẮT

Dưới sự phát triển của thời đại công nghệ số, các ứng dụng của khoa học kỹ thuật được áp dụng vào nhiều vào đời sống. Để đạt được sự phát triển đó đã có rất nhiều doanh nghiệp với kích thước vừa và nhỏ được lập nên, nhóm đối tượng mới này thường sẽ ưu tiên sử dụng công nghệ vào việc quản lý để có thể giảm thiểu chi phí nhất có thể. Vì vậy, nhóm chúng em quyết định tạo nên một mô hình quản lý tài nguyên mà nhóm doanh nghiệp vừa và nhỏ có thể áp dụng được. Đặc trương của mô hình này là sử dụng mạng nội bộ để kết nối các máy lại với nhau.

Dưới đây là mô hình mạng của hệ thống:

Về bản chất của mô hình này, các doanh nghiệp chỉ cần đầu tư vào 2 máy server và thiết bị giao tiếp giữa các thiết bị kết nối. Các client ở dưới không nhất thiết phải đặt cố định, cá thiết bị này có thể là các máy cá nhân.

# NỘI DUNG

## Giới thiệu tổng quan

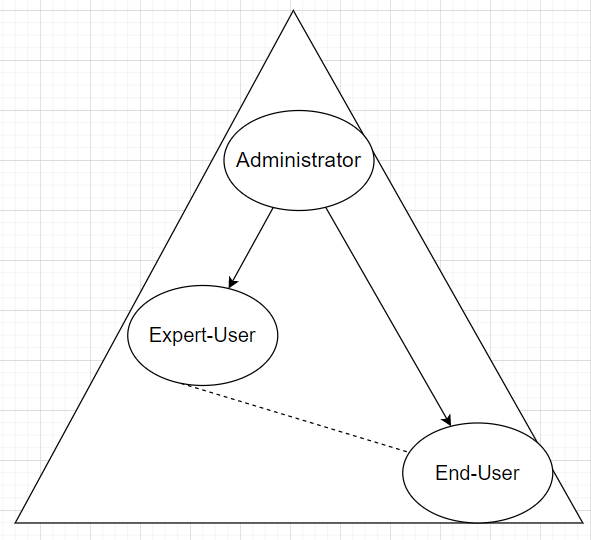
### Bảng IP

|  |  |  |  |
| --- | --- | --- | --- |
| Tên máy | Hệ điều hành | IP/subnetmask | Dich vụ |
| Server1 | Window Server 2012 | 192.168.1.2  255.255.255.0 | DNS, ADDS |
| Server2 | Window Server 2012 | 192.168.1.3  255.255.255.0 | ADDS, Webservice. |
| Client1 | Window | 192.168.1.20  255.255.255.0 |  |
| Client2 | Window | 192.168.1.21  255.255.255.0 |  |
| Client3 | Window | … |  |
| HackerMachine | Ubuntu | … |  |

Bảng 1: Bảng IP

### Mô hình OU.

|  |  |  |
| --- | --- | --- |
| Mức ưu tiên truy cập | Vị trí | Ý nghĩa |
| 1 | Administrator | Đây là nhóm OU có mức truy cập cao nhất, có khả năng truy cập vào máy chủ để kiẻm tra thông tin. |
| 2 | Expert-User | Là nhóm OU đặc thù, nhóm này cần một không gian lưu trữ riêng. |
| 3 | End-User | Là nhóm người dùng cuối cùng, nhóm này chỉ quản lý về mặt nhân viên. |

Bảng 2: Bảng OU

Hình 1: Mô hình phân cấp OU

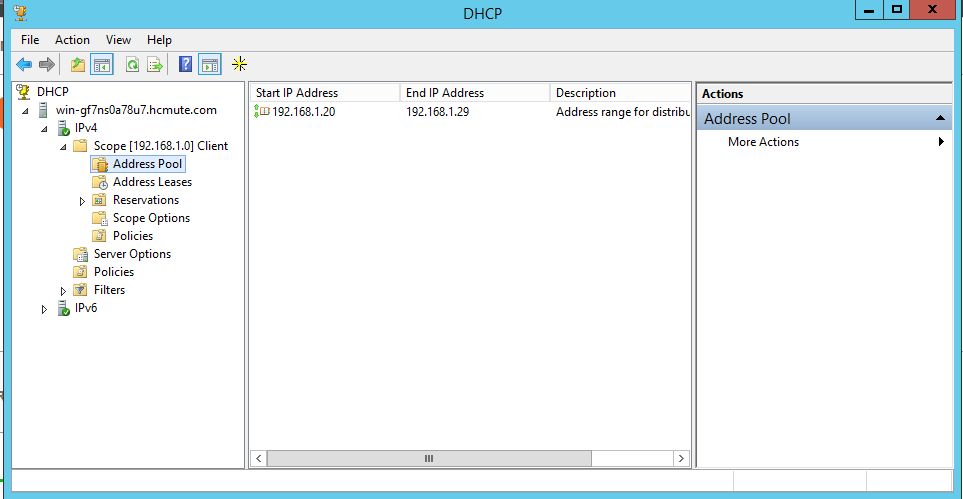
Các OU được phân cấp từ trên xuống dưới theo một hình tam giác càng lên cao thì mức độ ưu tiên của OU càng cao, và số lượng càng hạn chế lại. Và độ ưu tiên của OU được thiết lập theo mức độ ủy quền và các chính sách được ban ra cho từng OU.

### Kịch bản hoạt động.

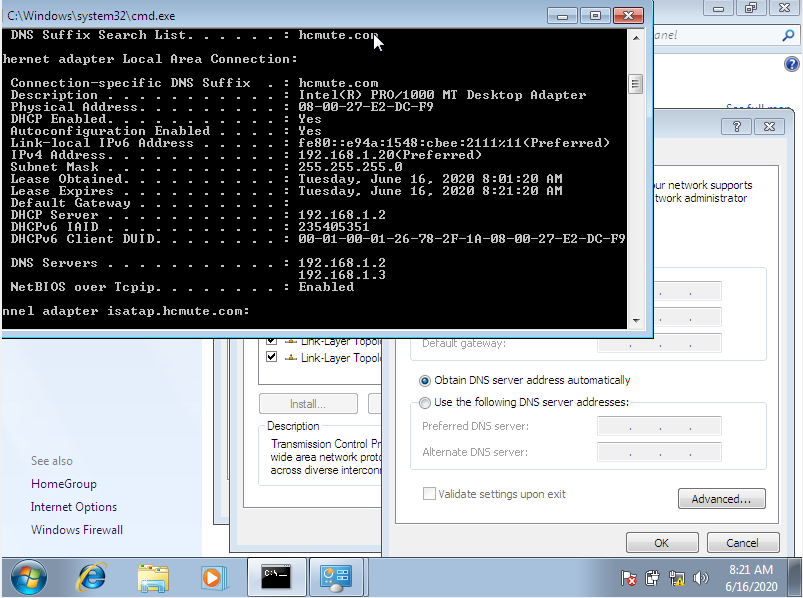
Khi bất kì một máy nào kết nối với mạng nội bộ của doanh nghiệp máy Server 1 sẽ nhận biết và dịch vụ DHCP sẽ tự nhận ra máy và cấp phát cho máy đó một IP để có thể hoạt động. Khi nếu chỉ là người dùng bình thường không phải là một nhân viên thì người này chỉ có thể truy cập vào dịch vụ webservice của hệ thống. Khi đăng nhập bằng nhập vào Domain, người dùng được coi là một thành phần của doanh nghiêp. Tùy vào vị trí và chức vụ người dùng sẽ được cấp một phần tài nguyên.

## Mô tả chi tiết.

### Dịch vụ DHCP.

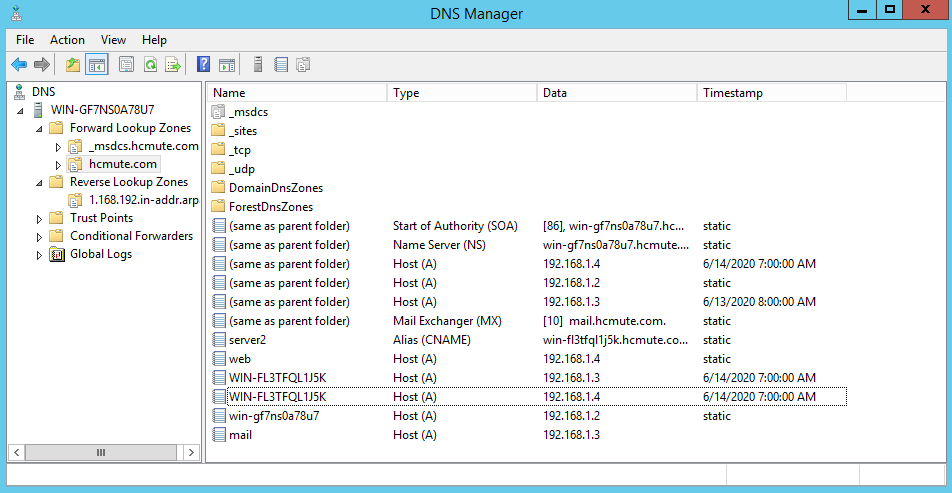
Sau khi cài đặt địch vụ DHCP, dịch vụ được cài đặt một Scope có mạng là [192.168.1]. Scope này được gọi là client vì bản chất nó sẽ cung cấp IP cho các máy con kết nối vào mạng nội bộ, các máy cố định như Server, các tài nguyên như máy in sẽ được đặt IP tĩnh hoặc được cấp bởi Reservation băng cách định danh địa chỉ vật lý.

Hình 2: Scope Client range

Kết quả thực nghiệm cho thấy DHCP hoạt động trong mức độ kiểm soát.

Hình 3: Kết quả khi kiểm thử DHCP

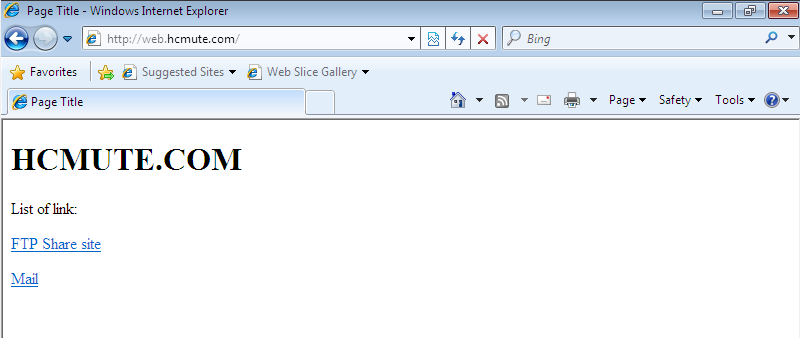
### Dịch vụ DNS và webservice.

Dịch vụ DNS được cài đặt trên máy server1 để trở thành nơi phân giải các IP được sử dụng trong hệ thống.

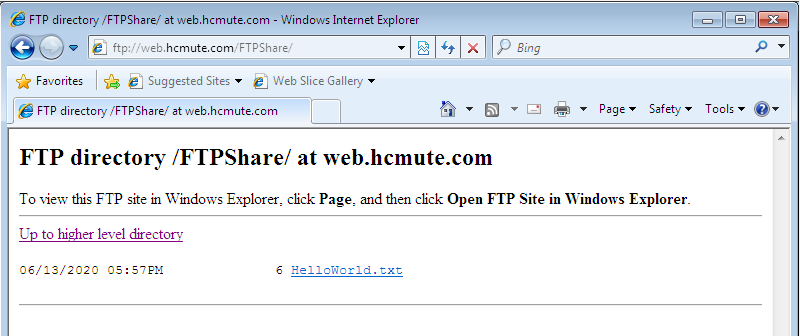
Hình 4: Danh sách DNS

Về phần WebService được cài đặt 2 site: 1 HTTP và 1 FTP. Trang http được tạo ra nhằm mục đính trở thành trang chủ cho các OU khi lên mạng cho thuận tiện, trang http này như là một list danh sách những dịch vụ web có thể sử dụng được. Còn về trang ftp đây trở thành một nơi để có thể lấy được các tài nguyên chia sẻ. Ngoài ra còn một dich vụ web nữa là mail, dịch vụ này trở thành một mail nội bộ để liên lạc được những nhân viên trong doanh nghiệp.

Kết quả về dịch vụ web:



Hình 5: Trang http.

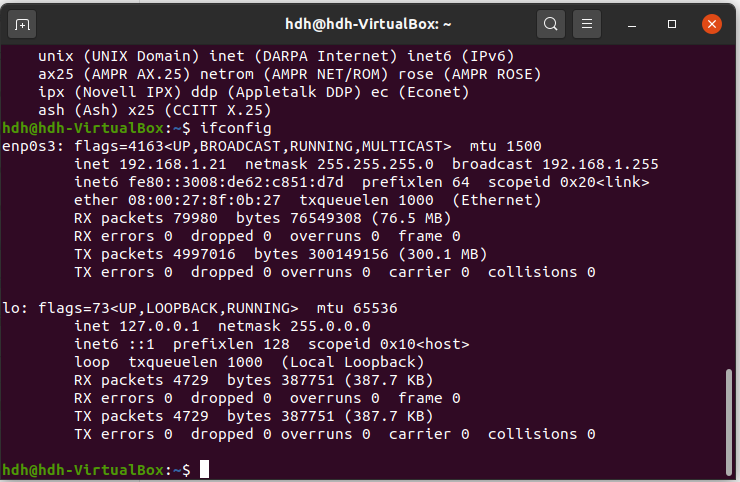


Hình 6: Trang ftp.

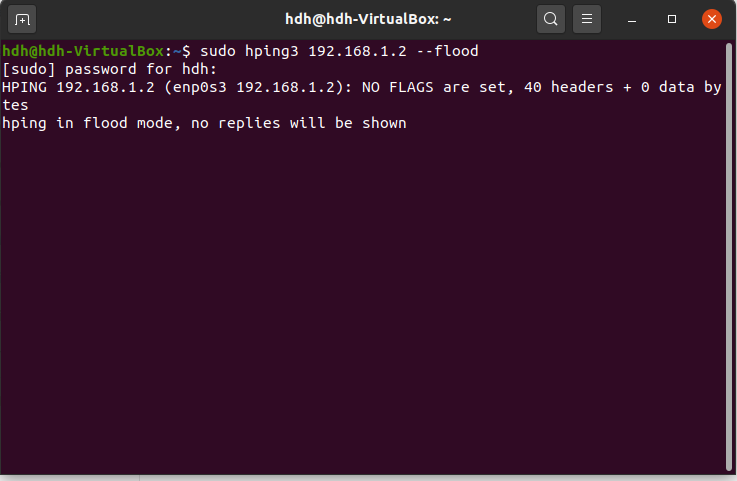
## Mô phỏng tấn công mạng

Công cụ: Hping3

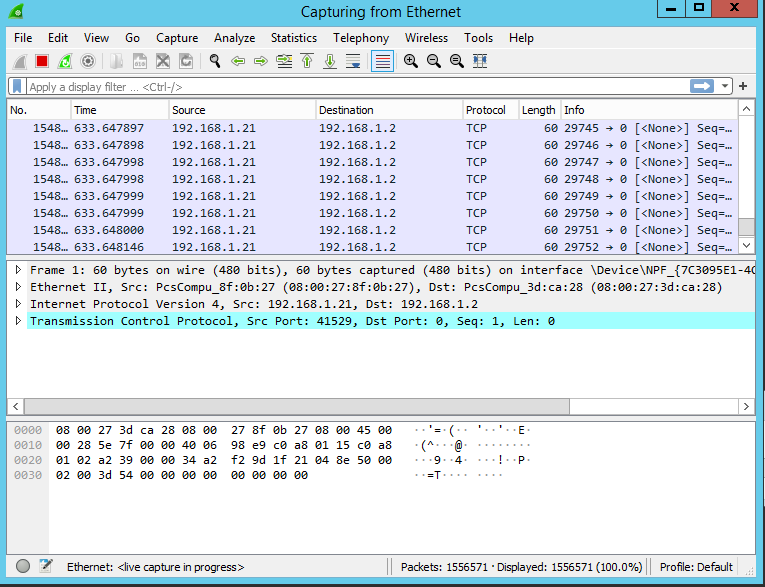
Phương thức: Flood.

Máy tấn công sẽ được kết nối vào mạng nội bộ của Server. Máy này sẽ vẫn được server nhận thức như một máy bình thường. Máy vẫn được cung cấp IP từ DHCP như bình thường. Sau đó máy sẽ được chạy lên tấn công lên server1 [192.168.1.2] dưới phương thức là Flood.

Hình 7: IP máy tấn công được Server cấp



Hình 8: Máy tấn công gây ngập

Khi đăng nhập vào máy bị tấn công (server1 [192.168.1.2]) và bật WireShark lên ta thấy hàng loạt các gói tin được gửi từ máy tấn công ([192.168.1.21]) dưới phương thức TCP, các gói tin được gửi đi mà máy server không kịp trả lời ngược lại. Ta có thể kết luận đây là tấn công từ chối dịch vụ theo phương thức flood.

Hình 9: WireShark bắt các gói tin

# KẾT LUẬN

## Ưu điểm.

Hiện tại hệ thống có thể hoạt động tốt, hệ thống đơn giản dễ dàng thiết lập, chi phí thấp, tiện lợi cho các doanh nghiêp mới bắt đầu hoặc các doanh nghiệp đang có ý định bắt đầu chuyển đổi số. Vì áp dụng hệ thống mạng nội bộ nên nếu có các cuộc tấn công diễn ra thì dễ dàng nắm bắt được.

## Nhược điểm.

Hệ thống nhỏ, thiết lập trên mạng nội bộ hoàn toàn nên không thể vừa truy cập vừa kết nối ra ngoài.

## Đề xuất cải tiến.

Hệ thống có thể đưa lên Microsoft Azure để có thể tiết kiệm tiền đầu tư thiết bị và bảo trì, ngoài ra còn được cung cấp các gói dịch vụ tốt hơn, các máy client có thể kết nối với mạng Internet bên ngoài.

# TÀI LIỆU THAM KHẢO

Hping3

<http://www.hping.org/manpage.html>

<https://www.howkteam.vn/course/certified-ethical-hacker-v10-vietnamese/102-tu-choi-dich-vu--cong-cu-tan-cong-dosddos-tan-cong-tran-syn-bang-metasploit--hping3-3861>