ĐH Khoa Học Tự Nhiên TP.HCM
Khoa Mạng Máy Tính
Bộ môn Chuyên đề Hệ điều hành Linux

BÁO CÁO ĐỒ ÁN THỰC HÀNH CUỐI KỲ

Học kỳ 1 - năm học 2018-2019

Danh sách thành viên

STT	MSSV	Họ và tên	Email	Số điện thoại
1	1312663	Nguyễn Minh Tuấn	nmtuan.dev@gmail.com	0934018329

Link phần bài nộp video:
https://drive.google.com/open?id=1g2_hY3vXTbV34G2xxkSm7OK9ApegXzlS

Kết quả hoàn thành

Mức độ hoàn thành dự tính: 90%

- ✓ Thiết kế network, phân chia subnet
- ✓ Cấu hình dịch vụ DHCP
- ✓ Cấu hình dịch vụ DNS
- ✓ Cấu hình dịch vụ Web
  - ✓ Static Website
  - ✓ Dynamic filesystem directory listing
  - ✓ Basic Auth
- ✓ Cấu hình dịch vụ SSH/SFTP
- ✓ Cấu hình firewall/router/http-proxy
- ✓ Cấu hình sample user host
- ✗ Cấu hình mail server

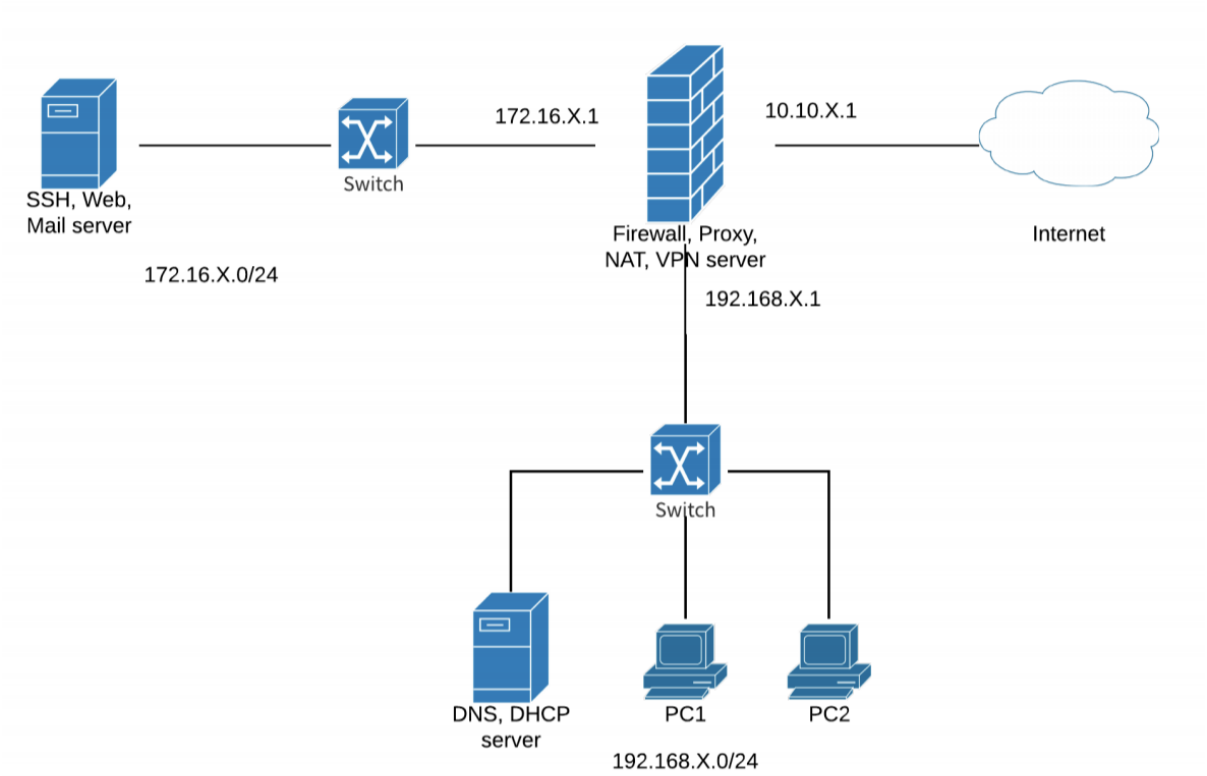
Lựa chọn công nghệ

Sau khi nghiên cứu và thử nghiệm nhóm em quyết định chọn Docker và Docker Compose làm công nghệ để thực hiện đồ án thực hành này.

Tổng quan về kiến trúc

Kiến trúc mạng của nhóm em thiết kế khá giống với yêu cầu đồ án đưa ra. Kiến trúc này gồm 2 subnet chính: Intranet và DMZ

Ngoài ra nhóm em còn thêm vào subnet Extranet để giả lập access đến từ bên ngoài.



Các subnet này được kết nối với nhau qua một bastion host. Bastion host này được cấu hình đồng thời như router, firewall và transparent HTTP proxy.

Cấu hình cụ thể

Toàn bộ các host trong bài thực hành này đều được chúng em cấu hình trên nền tảng Ubuntu 18.04 Docker container.

Ngoài ra Docker cũng tồn tại một số hạn chế như không thể khai báo default gw trên file compose. Để giải quyết chuyện này chúng em đã cài đặt bộ phần mềm net-tools và override default gw ở các host (trong Intranet và DMZ) để chúng trỏ tới Bastion host

```
# Replace docker default gateway so traffic will be routed to the bastion firewall
route del default
route add default gw 192.168.163.254 eth0 # Address of bastion host in intranet
```

Cấu hình DHCP Host

Để cái đặt DHCP host trên ubuntu thì chúng em phải cài gói phần mềm **isc-dhcp-server**

```
# Install dependencies
RUN apt-get update && apt-get install --yes \
  net-tools \
  isc-dhcp-server
```

Đề cấu hình dịch vụ DHCP thì chúng em phải chỉnh sửa nội dung của file **/etc/dhcp/dhcpd.conf**. Vì DHCP server này chỉ cần phục vụ cho các máy của user trong Intranet nên chúng em chỉ cần config cho duy nhất một subnet tương ứng

```
subnet 192.168.163.0 netmask 255.255.255.0 {
 range 192.168.163.10 192.168.163.190;
 option routers 192.168.163.1;
 option broadcast-address 192.168.163.255;
 default-lease-time 600;
 max-lease-time 7200;
}
```

Ngoài ra cấu hình default DNS server cũng được bọn em đặt trong file **/etc/dhcp/dhcpd.conf**

```
# option definitions common to all supported networks...
option domain-name "tuan.com";
option domain-name-servers 192.168.163.251;
```

DNS Host

Để cầu hình DNS host trên Ubuntu thì chúng em phải cài đặt các gói phần mềm bind.

```
# Install dependencies
RUN apt-get update && apt-get install --yes \
  net-tools \
  dnsutils \
  bind9 \
  bind9utils \
  bind9-doc
```

Đầu tiên chúng em phải cấu hình file **/etc/bind/named.conf.options** để khai báo các forwarder server tương ứng nếu DNS record không được tìm thấy.

```
forwarders {
  1.1.1.1;
  9.9.9.9;
  8.8.8.8;
};
```

Sau đó chúng em phải cấu hình file **/etc/bind/named.conf.local** để khai báo các DNS zone và các file database tương ứng của chúng. Ngoài zone chính cho domain của nhóm thì chúng em cũng khai báo các reverse lookup zone tương ứng với các subnet

```
zone "tuan.com" {
  type master;
  file "/etc/bind/zones/db.tuan.com";
};

zone "163.168.192.in-addr.arpa" {
  type master;
  file "/etc/bind/zones/db.192.168.163";
};

zone "163.16.172.in-addr.arpa" {
  type master;
  file "/etc/bind/zones/db.172.16.163";
};
```

Với mỗi zone thì chúng em sẽ phải cấu hình DNS record tương ứng trong file database đã được khai báo. Ví dụ file database của zone "tuan.com" ở **/etc/bind/zones/db.tuan.com**

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns.tuan.com. root.tuan.com. (
                              3         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.tuan.com.
@       IN      MX      0 mail.tuan.com.
ns      IN      A       192.168.163.251
@       IN      A       172.16.163.251
www     IN      A       172.16.163.251
ftp     IN      A       172.16.163.251
mail    IN      A       172.16.163.252
proxy   IN      A       192.168.163.1
```

Web Host

Web host mà chúng em cầu hình gồm có 2 phần chính
- NGINX server để phục vụ HTTP/HTTPS traffic.
- OpenSSH server để administrator có thể login và cấu hình các static file tương ứng

Để cấu hình NGINX thì trước hết chung em phải cài đặt gói phần mềm nginx. Sau đó chúng em phải chuẩn bị static web directory ở **/var/www/tuan.com** và nhúng cấu hình server tương ứng ở **/etc/nginx/sites-available/tuan.com**, symlink vào **/etc/nginx/sites-enabled/tuan.com** để enable site.

Đối với yêu cầu list file directory thì chúng em sử dụng tính năng autoindex của NGINX để hiện thị webpage như một filesystem directory

```
location /forum {
  autoindex on;
}
```

Đối với yêu cầu basic auth route thì trước tiên chúng em phải generate ra file .htpasswd cho admin user bằng công cụ **htpasswd** trong gói phần mềm **apache2-utils**. File này được đặt ở **/etc/nginx/.htpasswd** và sẽ được cấu hình để NGINX sử dụng làm basic auth database file

```
# Generate .htpasswd file for basic auth
RUN htpasswd -c -b /etc/nginx/.htpasswd ${ADMIN_USERNAME} ${ADMIN_PASSWORD}
```

```
location /admin {
  auth_basic           "Administrator's area";
  auth_basic_user_file /etc/nginx/.htpasswd;
}
```

Để setup SSL, ở đây chúng em chỉ sử dụng self-signed cert, đầu tiên chúng em phải generate ra cặp SSL key và cert bằng công cụ openssl

```
openssl req -x509 -nodes -days 3650 -newkey rsa:4096 -keyout site.key -out site.crt
```

Sau đó em phải cấu hình để NGINX phục vụ SSL traffic với cặp key và cert trên

```
listen 443 ssl default_server;
listen [::]:443 ssl default_server;
listen 4443 ssl default_server;
listen [::]:4443 ssl default_server;

root /var/www/tuan.com;

server_name tuan.com www.tuan.com;
ssl_certificate /etc/nginx/ssl/nginx.crt;
ssl_certificate_key /etc/nginx/ssl/nginx.key;
```

Để cấu hình dịch vụ SSH, thì chúng em phải cài gói phần mềm **openssh-server**. Và cấu hình file **/etc/ssh/sshd_config** theo yêu cầu của đề bài (PermitRootLogin no, …) Ngoài ra em cũng có cấu hình chỉ cho phép user SFTP lên thư mục **/var/www** và cấm shell access. Tuy nhiên để dễ test thì em comment phần này ra.

```
# Only allow these groups to gain SSH access
AllowGroups webadmin

# # Only allow webadmin to use sftp to manipulate /var/www directory without shell access
# Match Group webadmin
#   ForceCommand internal-sftp
#   PasswordAuthentication yes
#   ChrootDirectory /var/www
#   PermitTunnel no
#   AllowAgentForwarding no
#   AllowTcpForwarding no
#   X11Forwarding no
```

Bastion Host

Để cấu hình bastion host này đầu tiên chúng em phải cấu hình cho nó trở thành một network router. Với gói phần mềm net-tools chúng em có thể chỉnh sửa route table ở dưới Linux kernel. Ngoài ra chúng em còn phải enable kernal IP forwarding bằng lệnh **sysctl**

```
# Replace docker default gateway
route del default
route add default gw $INTERNET_GATEWAY $INTERNET_GATEWAY_INTERFACE

# Enable IP forwarding for routing
sysctl -w net.ipv4.ip_forward=1 > /dev/null 2>&1
```

Về firewall thì chúng em sử dụng công cụ iptables để cấu hình network như yêu cầu đồ án

```
#############################################################
# FILTER TABLE
#############################################################

# Set default policies to forbid all traffic
iptables -t filter -P INPUT DROP
iptables -t filter -P FORWARD DROP
iptables -t filter -P OUTPUT DROP

# Allow SSH from the intranet to anywhere
iptables -t filter -A FORWARD -s $INTRANET -p tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
iptables -t filter -A FORWARD -p tcp --sport 22 -m conntrack --ctstate ESTABLISHED -j ACCEPT

# Allow HTTP/HTTPS from anywhere to the dmz (where the web server is hosted)
iptables -t filter -A FORWARD -d $DMZ -p tcp -m multiport --ports 80,443 -j ACCEPT
iptables -t filter -A FORWARD -s $DMZ -p tcp -m multiport --ports 80,443 -j ACCEPT

# Allow HTTP/HTTPS from to the internet
iptables -t filter -A FORWARD -o $INTERNET_GATEWAY_INTERFACE -p tcp -m multiport --ports 80,443 -j ACCEPT
iptables -t filter -A FORWARD -i $INTERNET_GATEWAY_INTERFACE -p tcp -m multiport --ports 80,443 -j ACCEPT

# Allow DNS
iptables -t filter -A FORWARD -p tcp -m multiport --ports 53 -j ACCEPT
iptables -t filter -A FORWARD -p udp -m multiport --ports 53 -j ACCEPT

# DHCP shouldn't be allowed to pass through the firewall
# because the DHCP server sit in the same subnet as user machines
# thus connecting directly to each other
```

Để các máy trong mạng intranet có thể access được internet thì em cũng config các NAT rule tương ứng. Ngoài ra chúng em còn sử dụng và cấu hình Squid làm transparent HTTP proxy. Chúng em phải route các gói HTTP packet qua Squid server chạy chung với bastion host

```
#############################################################
# NAT TABLE
#############################################################

# Proxy HTTP/HTTPS traffic to squid
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT --to 127.0.0.1:3128

# Masquerade packet address to translate IP from/to the internet
iptables -t nat -A POSTROUTING -o $INTERNET_GATEWAY_INTERFACE -j MASQUERADE
```

Cấu hình squid tại **/etc/squid/squid.conf**

```
# Squid user:group
cache_effective_user proxy
cache_effective_group proxy

# Base config
http_port 3128

# Block websites
acl bad_url dstdomain .facebook.com

# ACLs
http_access deny bad_url
http_access allow all
```

User Host

Để cấu hình user host thì phần lớn chúng em phải cài các gói client phù hợp để tương tác với các dịch vụ.

```
# Install dependencies
RUN apt-get update && apt-get install --yes \
  net-tools \
  dnsutils \
  openssh-client \
  sshpass \
  iputils-ping \
  traceroute \
  iptables \
  nmap \
  curl
```

Ví dụ như gói nmap để gửi gói tin DHCP broadcast, gói dnsutils để kiểm tra DNS server, gói openssh client để kiểm tra cấu hình SSH…

Các script thực hiện cụ thể việc kiểm tra này được em đặt trong source code nộp kèm

Bảng phân công công việc

STT	Miêu tả công việc	Thành viên thực hiện	Phần trăm công việc
1	Nghiên cứu kiến trúc và lựa chọn công nghệ	1312663	10%
2	Cấu hình git và github repository	1312663	5%
3	Cấu hình hệ thống mạng và phân chia subnet	1312663	15%
4	Cấu hình dịch vụ DHCP	1312663	10%
5	Cấu hình dịch vụ DNS	1312663	10%
6	Cấu hình dịch vụ Web NGINX và SSH	1312663	20%
7	Cấu hình Bastion host routing/firewall/squid proxy	1312663	20%
8	Soạn tài liệu và viết báo cáo	1312663	10%

Tổng phân công:

1312663 - 100%