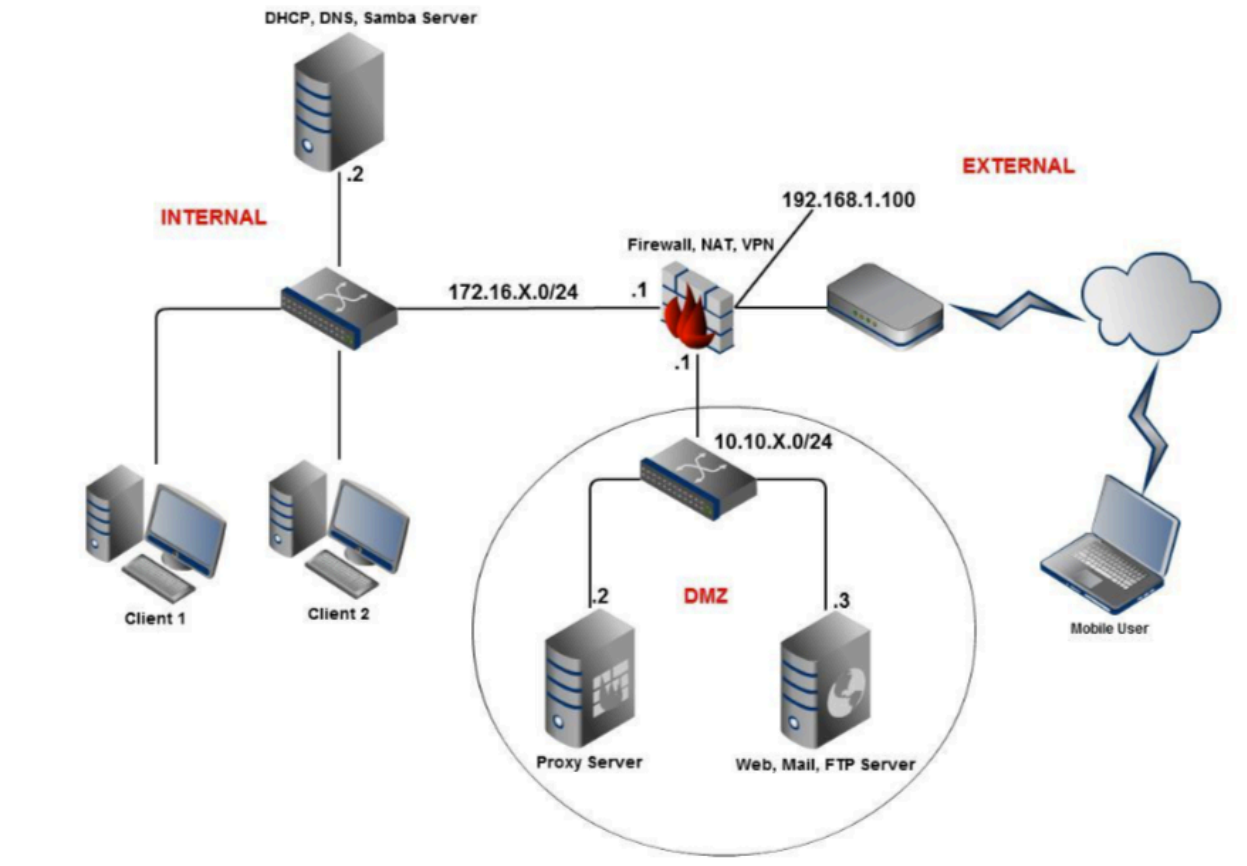
ĐỒ ÁN THỰC HÀNH MÔN HỌC

1. Mô hình



Đây là mô hình mạng firewall tri-homed để bảo vệ hệ thống bên trong với 3 vùng tách biệt (tham khảo thêm về mô hình DMZ trên Internet):

- INTERNAL: gồm các máy client và một số server, có đường mạng 172.16.X.0/24
- DMZ: gồm các server quan trọng được publish ra ngoài Internet, có đường mạng 10.10.X.0/24
- EXTERNAL: là mạng Internet. Công ty sở hữu một địa chỉ IP Public, ở đây ta dùng địa chỉ private 192.168.1.100 để giả lập. Khi triển khai trên máy ảo, 2 vùng INTERNAL và DMZ sẽ dùng 2 đường mạng tách biệt (như vmnet1

và vmnet2), còn vùng EXTERNAL sẽ dùng card mạng ở chế độ bridge.

Giá trị X ở trên được tính như sau: lấy MSSV của bạn có MSSV lớn nhất chia lấy dư cho 250. Ví dụ nhóm có 2 bạn là 0912300 và 091301 thì lấy 912301 chia lấy dư cho 250 được 51 => X = 51).

Công ty sở hữu domain có tên: XXXX.com, trong đó XXXX là tên của các bạn sinh viên trong nhóm. Ví dụ, nhóm gồm 2 sinh viên An, Bình thì domain là anbinh.com

2. Các dịch vụ

Lưu ý: Sinh viên có thể sử dụng các server Linux hoặc Windows hoặc kết hợp cả 2. Các phần mềm được nêu ra sau đây được gợi ý với môi trường Linux. Sinh viên có thể sử dụng phần mềm khác sao cho vẫn đảm bảo được các dịch vụ và các yêu cầu tính năng của dịch vụ đó cần cung cấp. Ví dụ: server NAT, Firewall, VPN trong mô hình có thể dùng Windows Server 2012 thay vì Linux server.

Các client có thể là Linux hoặc Windows.

2.1. Dịch vụ SSH

Tất cả các server trong mô hình này nếu là Linux đều phải cài đặt dịch vụ SSH để các client ở INTERNAL có thể truy cập và cấu hình các dịch vụ từ xa. Nếu là Windows Server thì cần được cài đặt dịch vụ Remote Desktop.

Chỉ cho phép remote từ INTERNAL. Không được login bằng tài khoản root thông qua SSH. Các tài khoản SSH trên DHCP, DNS server được chứng thực bằng username & password. Các tài khoản trên các server khác được chứng thực bằng SSH key-pair.

Cho phép chạy dịch vụ SFTP tương ứng với các tài khoản có quyền SSH.

2.2. DHCP, DNS & Samba

Cả 3 dịch vụ này cài đặt chung trên một máy 172.16.X.2/24

DHCP

Quản lý việc cấp phát IP trong phạm vi từ 172.16.X.50/24 đến 172.16.X.100/24 cho các máy trong mạng nội bộ công ty. DHCP Server phải loại trừ địa chỉ IP đã được đặt cho các server trong mạng INTERNAL. Địa chỉ DNS của các client phải được DHCP Server cung cấp để các máy tính trong công ty có thể truy cập dịch vụ của tất cả các server trong mạng và Internet.

DNS

Tên miền XXXX.com với XXXX là tên của các bạn sinh viên trong nhóm. Tạo các record:

- server2.xxxx.com có IP là 10.10.x.2
- server3.xxxx.com có IP là 10.10.x.3
- proxy.xxxx.com là alias của server2
- www.xxxx.com, ftp.xxxx.com, mail.xxxx.com là alias của server3

Samba

Triển khai Samba server gồm các yêu cầu sau:

- Tạo group “ketoan”: gồm các user kt1, kt1
- Tạo group “nhanvien”: gồm các user nv1, nv2
- Share thư mục /data/ketoan cho group “ketoan (các user thuộc group này được full quyền trên thư mục này)

- Share thư mục /data/nhanvien cho group “nhanvien” (các user thuộc group này được full quyền)
- Share thư mục /data/dulieuchung cho guest nhưng chi có đọc.

2.3. **Web, FTP & Mail**

Cả 3 dịch vụ này cài đặt chung trên một máy 10.10.X.3/24

Lưu ý: Các dịch vụ này khi kiểm tra hoạt động cần phải kiểm tra truy cập từ cả 2 vùng INTERNAL và EXTERNAL.

Web

Xây dựng một website với Wordpress (https://wordpress.org/). Ứng với dữ liệu mẫu khi cài đặt Wordpress. Và các máy Internal có thể truy cập thông qua tên miền www.xxxx.com

- Thư mục cài đặt web sẽ là /var/www/xxxx.com
- Yêu cầu cài đặt gồm có Apache, PHP và MySQL

Lưu ý: Sinh viên có thể sử dụng web server Apache hoặc nginx nếu dùng Linux.

FTP

Triển khai FTP server dùng vsftp với các yêu cầu sau:

- Chỉ cho phép người dùng anonymous truy cập vào FTP Server. Và thư mục gốc của FTP Server dành cho người dùng anonymous là /data/anon/ftp
- Người dùng anonymous không có quyền upload nội dung lên FTP Server, chỉ có quyền download nội dung về
- Tạo 2 user sv1/123456, sv2/123456. Cấu hình chroot để các tài khoản này không thể truy cập các thư mục khác ngoài thư mục /var/www/xxxx.com

Mail

Thiết lập Mail server như sau:

- SMTP server sử dụng Sendmail hoặc Postfix
- POP3/IMAP Server sử dụng Dovecot
- Cho phép gửi/nhận mail qua Web (Webmail) sử dụng squirrelmail
- Tích hợp chức năng lọc spam mail với Spam Assassin, quét virus với Clamav

Lưu ý: Sinh viên có thể cài đặt và sử dụng mail server khác, ví dụ: iRedMail, mdeamon

2.4. **Proxy & VPN**

Proxy

Sử dụng Squid để triển khai chức năng transparent proxy. Người sử dụng không cần phải cấu hình để sử dụng proxy. Tất cả các truy cập của người dùng từ mạng nội bộ đi ra Internet đều phải thông qua proxy server, tuy nhiên người sử dụng không hề biết sự tồn tại của proxy này trong hệ thống. Ngoài ra, proxy còn có điều khiển truy cập như sau: Cấm không cho truy cập vào các trang facebook.com, twitter.com trong giờ làm việc (9:00 AM – 17:00 PM).

VPN

Dùng OpenVPN để triển khai mô hình Client-To-Site cho phép các user có thể quay VPN và truy cập vào mạng công ty.

2.4. Firewall & NAT

Firewall được giả lập là một server chạy HĐH Linux gồm 3 card mạng có IP như

trên mô hình và có cài đặt IPTables. Firewall có các chức năng sau:

Routing

Cho phép các máy trong INTERNAL có thể connect đến vùng DMZ.

NAT

Forward các traffic từ vùng EXTERNAL (gồm các traffic HTTP, HTTPS, SMTP, POP3, FTP) đi vào các server trong vùng DMZ.

Forward các traffic từ INTERNAL đi ra EXTERNAL.

Firewall rules

Các máy từ DMZ không được phép connect vào các máy trong INTERNAL (chỉ reply lại request).

Các máy từ EXTERNAL không được phép connect vào các máy trong INTERNAL (chỉ reply lại request).

3. Bài nộp

Bài làm được thực hiện theo nhóm tối đa 4 sinh viên. Sinh viên được quyền tự chọn nhóm thực hiện.

Nghiêm cấm mọi hành vi chép kết quả lẫn nhau. Nếu phát hiện có sự gian lận, cả nhóm chép và cho chép đều bị điểm 0 cho phần thực hành này.

Nếu có sự tham khảo để thực hiện đồ án này, sinh viên phải nêu rõ nguồn tham khảo trong báo cáo và tập tin cấu hình.

Tập tin cấu hình được chú thích rõ ràng tại các dòng do nhóm thực hiện, hoặc chỉnh sửa.

Hình thức nộp

Nộp qua trang Moodle môn học theo các mốc thời gian: lần 1, lần 2... Ứng với mỗi lần nộp, các dịch vụ được tích hợp dần vào mô hình, viết báo cáo cho các nội dung đã thực hiện. Ví dụ: lần 1 cần tích hợp và viết báo các cho việc thiết lập mô hình và tích hợp các dịch vụ SSH, DNS, DHCP.

Bài làm được nén thành 1 file zip với tên là mã số sinh viên của các thành viên "MSSV1-MSSV2….zip".

Cấu trúc file bài nộp:

- Báo cáo: dạng "MSSV1-MSSV2….pdf". Trong báo cáo, nhóm phải nêu rõ giải pháp, các bước cấu hình (chỉ chụp hình các bước cấu hình chính cho thấy rõ yêu cầu). Ngoài ra báo cáo phải có bước kiểm tra hoạt động của dịch vụ sau khi cấu hình.
- Thư mục "config" chứa toàn bộ các tập tin cấu hình cho từng dịch vụ. Các thư mục con được tạo ra tương ứng với từng dịch vụ để chứa các tập tin cấu hình tương ứng. Ví dụ: config/dhcp, config/dns

4. Tham khảo

- Các tài liệu hướng dẫn thực hành
- Từ khóa: linux, dmz, iptables, nat
- https://www.server-world.info
- https://www.digitalocean.com
- https://hocvps.com/