Môn học Thực tập cơ sở

Bài 5: Cài đặt, cấu hình mạng doanh nghiệp với Pfsense firewall

1.1 Mục đích

Các công ty thường bảo vệ hệ thống mạng bằng cách sử dụng tường lửa phần cứng hoặc phần mềm để kiểm soát lưu lượng mạng truy cập. Một số loại lưu lượng nhất định có thể bị chặn hoặc cho phép đi qua tường lửa. Việc hiểu cách thức hoạt động của tường lửa và mối quan hệ của nó với các mạng bên trong và bên ngoài sẽ rất quan trọng để có hiểu biết về bảo mật mạng.

Bài thực hành này giúp sinh viên có thể tự cài đặt, xây dựng một mạng doanh nghiệp với tường lửa để kiểm soát truy cập. Mạng mô phỏng môi trường mạng doanh nghiệp này có thể sử dụng trong các bài lab về ATTT sau này.

1.2 Nội dung thực hành

1.2.1 Tìm hiểu lý thuyết

- Tìm hiểu về cấu hình mạng trong phần mềm mô phỏng Vmware/Virtualbox
  - Sinh viên đọc tài liệu tham khảo:

    - Vmware Workstation Networking Overview: https://masteringvmware.com/vmware-workstation-networking-overview/

    - Network in VMware Workstation: https://github.com/ducnc/vmware-workstation-network

    - VirtualBox Network Settings: Complete Guide: https://www.nakivo.com/blog/virtualbox-network-setting-guide/
- Tài liệu tham khảo:

  - Lab 7 pfsense firewall của CSSIA CompTIA Security+®

  - Advanced Penetration Testing for Highly-Secured Environments Second Edition

- Giới thiệu về Pfsense: https://viblo.asia/p/network-gioi-thieu-ve-pfsense-N0bDM6LXv2X4

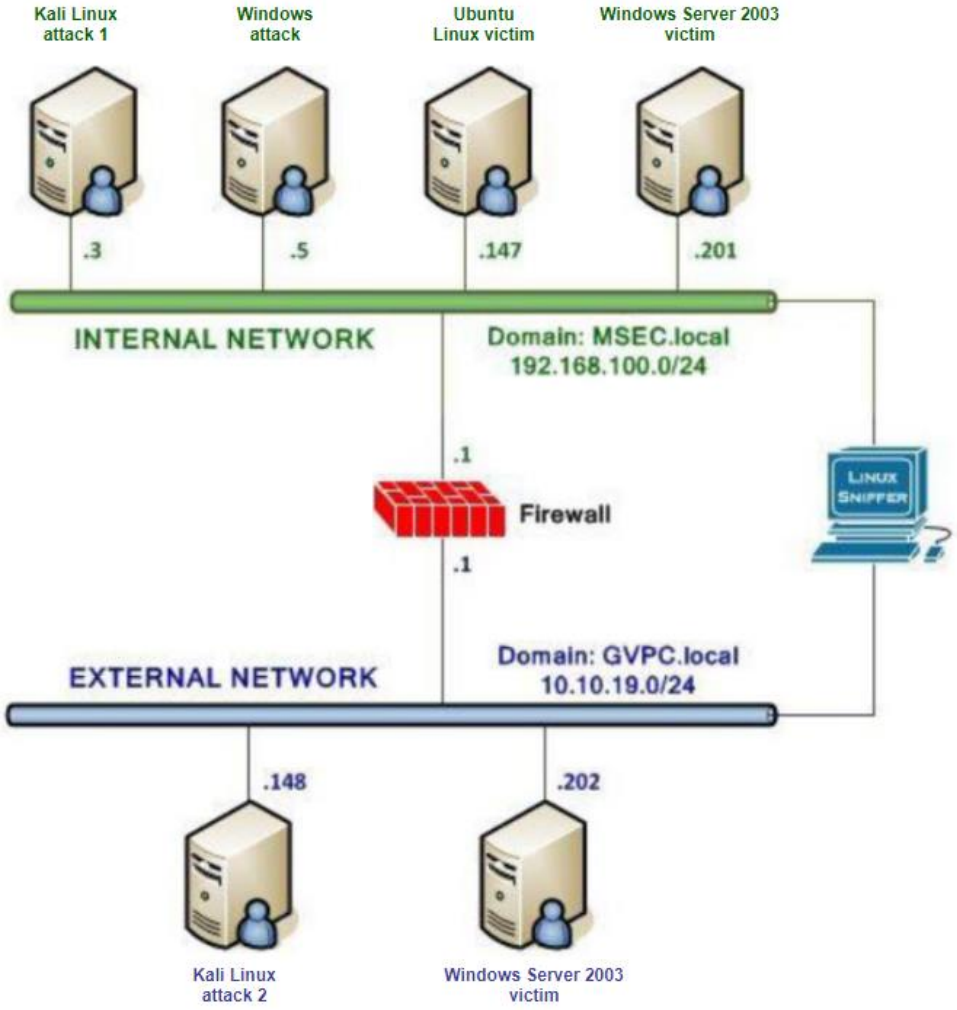
1.2.2 Chuẩn bị môi trường

- Phần mềm VMWare Workstation.
- Các file máy ảo VMware đã cài đặt trong các bài lab trước đó: máy trạm, máy chủ Windows và Linux.
- File cài đặt tường lửa Pfsense

1.2.3 Các bước thực hiện và kết quả cần đạt

1.2.3.1 Cấu hình topo mạng

a) Cài đặt và cấu hình hệ thống theo topo mạng và thông tin như mô tả dưới đây (bao gồm cài đặt các máy ảo)



Thông tin yêu cầu cho các thiết bị trong hệ thống:

Máy Kali Linux attack 1 trong mạng Internal	IP: 192.168.100.3 Mật khẩu root: password
Máy Windows Server 2003 Victim trong mạng Internal	IP: 192.168.100.201 Mật khẩu root: password
Máy Linux Victim trong mạng Internal	IP: 192.168.100.147 Mật khẩu root: password
Máy pfSense Firewall	IP: 10.10.19.1, 192.168.100.1 Mật khẩu: admin/pfsense
Máy Linux Attack trong mạng External	IP: 10.10.19.148 Mật khẩu root: password
Máy Windows Server 2003 Victim trong mạng External	IP: 10.10.19.202 Mật khẩu root: password

Chú ý: nếu không tìm được phiên bản Windows Server 2003 thì sinh viên có thể sử dụng các phiên bản Windows Server khác cho bài này.

b) Kết quả cần đạt được

- Cài đặt, cấu hình địa chỉ IP thành công, các máy trong mạng ping được nhau.
- Chú ý: đối với các máy yếu, chỉ có thể chạy được một số ít các máy ảo đồng thời thì sinh viên chạy thử nghiệm tương ứng đủ số máy cần thiết, các máy không cần tắt đi để đỡ ảnh hưởng đến hiệu năng tổng thể của máy tính.

1.2.3.2 Cài đặt cấu hình pfsense firewall cho lưu lượng ICMP

a) Cấu hình ICMP cho phép các máy trong mạng Internal ping được ra các máy ở mạng External, không cho phép ping vào trong mạng Internal. Các bước lần lượt như sau:

- Trên máy Linux victim ở mạng trong, vào http://192.168.100.1 để cấu hình pfsense qua giao diện web.

- Cấu hình luật firewall để cho phép luồng ICMP ở mạng External ping được tới giao diện 10.10.19.1
- Kiểm tra bằng cách ping tới 10.10.19.1 từ máy Kali attack ở mạng ngoài.

b) Kết quả cần đạt được

- Cài đặt, cấu hình thành công. Các máy đều cần có user với tên "tên sinh vien_mã sinh viên".
- Chụp ảnh các bước thực hiện và mô tả trong báo cáo cùng với lý thuyết có liên quan.
- Trả lời câu hỏi:
  - Theo mặc định, có bao nhiêu cổng TCP mở trên giao diện mạng trong của pfSense?
  - Theo mặc định, có bao nhiêu cổng TCP mở trên giao diện mạng ngoài của pfSense?
- Minh chứng
  - Thực hiện các lệnh ping như trên trong cửa sổ cmd
  - In ra màn hình tên người dùng (trong Windows là lệnh echo %USERNAME%) và ngày tháng năm thực hiện (lệnh date)

1.2.3.3 Cài đặt cấu hình pfsense firewall cho phép chuyển hướng lưu lượng tới các máy trong mạng Internal

a) Cấu hình tường lửa cho phép 1 cổng và chuyển hướng lưu lượng:

- Trên máy Linux victim ở mạng trong, vào http://192.168.100.1 để cấu hình NAT trên pfsense qua giao diện web.
- Cấu hình cho phép cổng SSH trên IP 192.168.100.147 (Máy Linux victim mạng Internal) được truy cập từ bên ngoài thông qua port forwarding. Nghĩa là khi các máy khách từ mạng 10.10.19.0/24 kết nối với địa chỉ IP của tường lửa pfSense của 10.10.19.1, chúng sẽ được chuyển hướng đến máy Linux victim trong mạng Internal.
- Kiểm tra bằng cách truy cập ssh tới 10.10.19.1, rồi gõ ifconfig để kiểm tra IP máy có phải là 192.168.100.147 hay không?

- Kiểm tra các cổng được phép truy cập trên mạng Internal bằng cách gõ lệnh trên máy Kali Linux trong mạng Internal: nmap 192.168.100.1

b) Kết quả cần đạt được

- Cài đặt, cấu hình thành công. Các máy đều cần có user với tên "tên sinh vien_mã sinh viên".
- Chụp ảnh các bước thực hiện và mô tả trong báo cáo cùng với lý thuyết có liên quan.
- Minh chứng

    a. Thực hiện các lệnh trong như trong hướng dẫn các bước thực hiện bên trên và chụp ảnh minh chứng

    b. In ra màn hình tên người dùng (trong Windows là lệnh echo %USERNAME%) và ngày tháng năm thực hiện (lệnh date)

1.3 Yêu cầu đối với file báo cáo

- File báo cáo dưới dạng pdf được trình bày rõ ràng theo cấu trúc: trang bìa, mục lục, các phần lý thuyết và thực hành riêng, tài liệu tham khảo nếu có. Báo cáo được đánh số trang trừ trang bìa.
- Đặt tên file theo định dạng kiểu như sau: *Bài thực hành 5_Họ tên SV_Mã SV*