Môn học Thực tập cơ sở

Bài 9: Phân tích log hệ thống

1 Mục đích

Bài thực hành này giúp sinh viên nắm được công cụ và cách phân tích log hệ thống, bao gồm:

1. Phân tích log sử dụng grep/gawk trong Linux
2. Phân tích log sử dụng find trong Windows
3. Tìm hiểu về Windows Event Viewer và auditing
4. Phân tích event log trong Windows

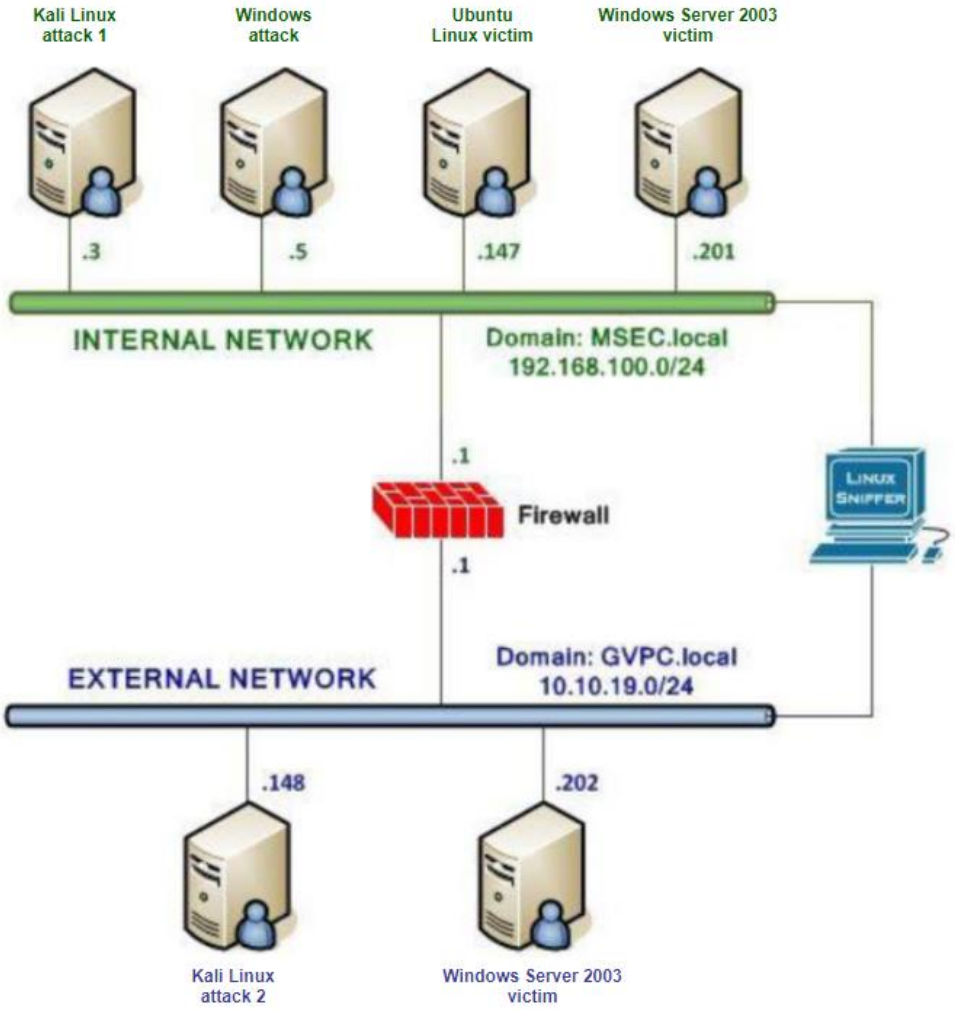
2 Nội dung thực hành

2.1 Tìm hiểu lý thuyết

- Tìm hiểu về ý nghĩa của một số lệnh dùng cho quá trình phân tích log: grep, gawk, find, secure, access_log, …
- Tài liệu tham khảo:
  - grep: https://linuxcommand.org/lc3_man_pages/grep1.html
  - gawk: http://www.gnu.org/software/gawk/manual/gawk.html
  - find:https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/find
  - xhydra: http://manpages.ubuntu.com/manpages/bionic/man1/hydra.1.html

2.2Chuẩn bị môi trường

- Phần mềm VMWare Workstation (hoặc các phần mềm hỗ trợ ảo hóa khác).
- Các file máy ảo VMware và hệ thống mạng đã cài đặt trong bài lab 05 trước đó: máy trạm, máy Kali Linux, máy chủ Windows và Linux. Chú ý: chỉ cần bật các máy cần sử dụng trong bài thực hành.
- Topo mạng như đã cấu hình trong bài 5.



2.3Các bước thực hiện và kết quả cần đạt

2.3.1 Phân tích log sử dụng grep trong Linux

a) Các bước thực hiện

- Trên máy Kali attack trong mạng Internal, khởi chạy zenmap và scan cho địa chỉ **192.168.100.147**(Máy Linux victim) và xem được port 80 đang mở cho Web Server Apache 2.2.3
- Trên máy Kali attack ở mạng Internal, truy cập địa chỉ web http://192.168.100.147. Trên terminal tiến hành sao chép website và tìm kiếm từ khóa "test"(root@bt:~#**curl http://192.168.100.147 grep test)**
- Trên máy Linux Internal Victim, để xem thư mục chứa ***access_log*** dùng lệnh: [root@rhel ~]# **cd /var/log/httpd**

b) Kết quả cần đạt được

- Khi đã mở được file ***access_log*** trên máy nạn nhân, dùng grep để lọc ra kết quả với một số từ khóa tìm kiếm ví dụ: Nmap, Firefox, curl, …
- Minh chứng:

  - Chụp ảnh minh chứng kết quả lọc dữ liệu dùng grep trên file log của máy nạn nhân, cần chụp được phần tên máy có chứa tên và mã sinh viên.

2.3.2 Phân tích log sử dụng gawk trong Linux

a) Các bước thực hiện

- Trên máy Kali attack tiến hành remote vào máy Linux Internal Victim. Tạo một account mới với tên sinh viên và mật khẩu tùy chọn. Sau đó tiến hành thay đổi mật khẩu cho tài khoản vừa tạo.
- Trên máy Linux Internal Victim, tiến hành xem file log
- Trên máy Kali attack, thông qua chế độ remote tiến hành tìm kiếm những người dùng vừa tạo bằng lệnh grep, và dùng lệnh gawk để in một hoặc nhiều dòng dữ liệu tìm được.

b) Kết quả cần đạt được

- Xem được log và tìm được nội dung mong muốn bằng lệnh grep/gawk. In được kết quả mong muốn lên màn hình.
- Minh chứng:

  - Chụp ảnh minh chứng thông tin các người dùng tạo thêm phải có tên/mã sinh viên, và in được kết quả tìm kiếm bằng lệnh gawk tương ứng.

2.3.3 Phân tích log sử dụng find trong Windows

a) Các bước thực hiện

- Trên máy Kali External Attack khởi động #xhydra, chọn target là **10.10.19.202**, giao thức ftp và cài đặt Password list, sau đó nhấn Start và chờ xHydra tìm ra mật khẩu
- Trên máy Windows 2003 Server External Victim, thực hiện điều hướng đến FTP Logfile(C:**cd c:\Windows\System32\Logfiles\msftpsvc1)**. Chọn hiển thị tất cả các file log đang có và chọn 1 file mới nhất để mở ra (ngày tháng có dạng yymmdd). Gõ lệnh để tìm kiếm kết quả tấn công login thành công(C:\WINDOWS\system32\LogFiles\MSFTPSVC1>**type ex**yymmdd**.log | find "230")**

b) Kết quả cần đạt được

- Lưu được dữ liệu log tấn công mật khẩu và tìm được kết quả tấn công trong file log trên máy victim.
- Thực hiện viết báo cáo cho bài thực hành theo các bước đã mô tả bên trên.
- Minh chứng:

  - Chụp ảnh kết quả trong folder FTP Logfile sau khi tấn công, và mở được file log ngày tháng thực tế mà sinh viên tiến hành thử nghiệm.

3 Các yêu cầu với báo cáo bài thực hành

Báo cáo bài thực hành cần có đầy đủ các nội dung/thành phần sau:

- Trang bìa (ghi rõ môn học, bài thực hành, mã sv và họ và tên.
- Trình bày vắn tắt về các nội dung lý thuyết đã tìm hiểu được trong mục 2.1(từ 2-5 trang)
- Các nội dung thực hành cần kèm ảnh minh chứng theo thứ tự thực hiện các bước.
- Đặt tên file theo định dạng kiểu như sau: *Bài thực hành 9_Họ tên SV_Mã SV*