|  |
| --- |
| HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG  **KHOA CÔNG NGHỆ THÔNG TIN 1** |
|  |
| **BÀI THỰC HÀNH 9**  **THỰC TẬP CƠ SỞ** |
| **Họ và tên : Đinh Quang Hiếu**  **Mã sinh viên: B19DCAT065**  **Giảng viên giảng dạy: Hoàng Xuân Dậu** |
| **HÀ NỘI, THÁNG 3/2022** |

# Bài 9: Phân tích log hệ thống

1. **Giới thiệu chung**
   1. **Mục đích**

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

# Yêu cầu

* Tìm hiểu lý thuyết
  + Grep: là command hiển thị line chứa chuỗi kí tự trong file .Có thể chỉ định nhiều file hoặc nhiều đường dẫn của đối tượng search . Có thể thay file hoặc đường dẫn bằng kết quả output từ command khác
  + Awk: là một ngôn ngữ lập trình hỗ trợ thao tác dễ dàng đối với kiểu dữ liệu có cấu trúc, thường được sử dụng cho việc tìm kiếm và xử lý text. Gawk là bản phát hành mới nhất của GNU awk
  + Find được sử dụng để tìm kiếm một chuỗi văn bản trong một tệp hoặc các tệp và hiển thị các dòng văn bản chứa chuỗi đã chỉ định trong cmd Windows
  + Access\_log:
    - Có chức năng ghi lại những lần sử dụng, truy cập, yên cầu đến apache server;
    - Được lưu trữ tại /var/log/httpd/access\_log (hoặc /var/log/apache2/access.log)
  + xHydra:
    - xHydra là giao diện người dùng GUI cho trình bẻ khóa mật khẩu Hydra.
    - Hydra có thể được sử dụng để bẻ khóa mật khẩu, có thể được sử dụng cho nhiều loại tấn công trực tuyến, bao gồm cả các cuộc tấn công MySQL, SMB, FTP, MSSQL và HTTP / HTTPS.

* Chuẩn bị
  + Phần mềm VMWare Workstation
  + File máy ảo VMware và hệ thống mạng đã cài đặt trong bài lab 5
  + Topo mạng như đã cấu hình trong bài 5
  1. Các bước thực hiện

+ Phân tích log sử dụng grep trong Linux

1. 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

Graphical user interface, text

Description automatically generated

* + Trên máy Kali attack ở mạng Internal, truy cập địa chỉ web [http://192.168.100.147](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**](http://192.168.100.147/)**| grep test)**

Graphical user interface, text

Description automatically generated

Graphical user interface

Description automatically generated

* Trên máy Linux Internal Victim, để xem thư mục chứa ***access\_log*** dùng lệnh: [root@rhel ~]# **cd /var/log/apache2/**

Text

Description automatically generated

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, …
* Grep Nmap access.log

Text

Description automatically generated

* Grep Firefox access.log

Text

Description automatically generated

* Grep curl access.log

Text

Description automatically generated

+ Phân tích log sử dụng gawk trong Linux

1. *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.

Text

Description automatically generated

Text

Description automatically generated

* + Trên máy Linux Internal Victim, tiến hành xem file log

gedit /var/log/auth.log

Text

Description automatically generated

* + 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.

Text

Description automatically generated with medium confidence

A picture containing graphical user interface

Description automatically generated

+ Phân tích log sử dụng find trong Windows

1. 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

Graphical user interface, application

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Text

Description automatically generated

* + Trên máy Windows Server External Victim, thực hiện điều hướng đến FTP Logfile(C:\**cd C:\inetpub\logs\Logfiles\FTPSVC3)**. Chọn hiển thị tất cả các file log đang có và chọn 1 file mới nhất để mở ra (ngày tháng có dạng yymmdd)

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text

Description automatically generated

Graphical user interface, text, application

Description automatically generated