

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÁO CÁO BÀI THỰC HÀNH THỰC TẬP CƠ SỞ

Bài 9: Phân tích log hệ thống

# Họ và tên: Nguyễn Huy Quang

# Mã sinh viên: B20DCAT144

**Giảng viên: Nguyễn Hoa Cương**

***Hà Nội – 2023***

MỤC LỤC

1. [Tìm hiểu lý thuyết 1](#_TOC_250009)
   1. [find 1](#_TOC_250008)
   2. grep 1
   3. xhydra 2
   4. gawk 3
2. [Nội dung thực hành 3](#_TOC_250007)
   1. [Chuẩn bị môi trường 3](#_TOC_250006)
   2. [Các bước thực hành 4](#_TOC_250005)
      1. [Phân tích log sử dụng grep trong Linux 4](#_TOC_250004)
      2. [Phân tích log sử dụng gawk trong Linux 10](#_TOC_250003)
      3. [Phân tích log sử dụng find trong Windows 13](#_TOC_250002)
3. [Tổng kết 17](#_TOC_250001)
4. [Tài liệu tham khảo 18](#_TOC_250000)

# Tìm hiểu lý thuyết

Ý nghĩa một số lệnh dùng trong quá trình phân tích log: find, xhydra, gawk, grep

# find

* + - Tìm kiếm một chuỗi văn bản trong một tệp hoặc các tệp và hiển thị các dòng văn bản chứa chuỗi đã chỉ định.
    - Cú pháp:

*find [/v] [/c] [/n] [/i] [/off[line]] <"string"> [[<drive>:][<path>]<filename>[...]]*

|  |  |
| --- | --- |
| Tham số | Mô tả |
| /v | Hiển thị tất cả các dòng không chứa <string> được  chỉ định. |
| /c | Đếm các dòng có chứa <string> được chỉ định và hiển  thị tổng số |
| /n | Đặt trước mỗi dòng với số dòng của file |
| /i | Chỉ định rằng tìm kiếm không phân biệt chữ hoa chữ  thường. |
| [/off[line]] | Không bỏ qua các file đã đặt thuộc tính ngoại tuyến. |
| <”string”> | Chỉ định nhóm ký tự (được đặt trong dấu ngoặc kép)  muốn tìm kiếm |
| [<drive>:][<path>]<filename> | Chỉ định vị trí và tên của file để tìm kiếm chuỗi được  chỉ định. |

vd: find “pencil sharpener” pencil.md

Ý nghĩa: Hiển thị tất cả các dòng trong *pencil.md* mà chứa chuỗi *pencil sharpener*

* 1. **grep**
     + grep tìm kiếm “mẫu” trong mỗi file.”Mẫu” là một hoặc các mẫu được phân tách bằng ký tự dòng mới và grep in từng dòng khớp với một mẫu.
     + FILE của “-” là viết tắt của đầu vào tiêu chuẩn. Nếu không có FILE nào được đưa ra, các tìm kiếm đệ quy sẽ kiểm tra thư mục đang làm việc và các tìm kiếm không đệ quy đọc đầu vào chuẩn.
     + Cú pháp:

*grep [option] PATTERNS [FILE…]*

|  |  |
| --- | --- |
| Tùy chọn | Mô tả |
| -E (--extended-regexp) | Diễn giải MẪU dưới dạng biểu thức  chính quy mở rộng |
| -F (--fixed-strings) | Giải thích MẪU dưới dạng chuỗi cố định,  không phải biểu thức chính quy.) |
| -G (--basic-regexp) | Diễn giải MẪU dưới dạng biểu thức  chính quy cơ bản (mặc định) |
| -P (--perl-regexp) | Diễn giải MẪU dưới dạng biểu thức chính quy tương thích với Perl (PCRE). Tùy chọn này là thử nghiệm khi được kết hợp với tùy chọn -z (--null-data) và grep - P có thể cảnh báo về các tính năng chưa  được thực hiện. |

* 1. **xhydra**
     + Hydra là một trình bẻ khóa đăng nhập song song hỗ trợ nhiều giao thức để tấn công. Các mô-đun mới rất dễ thêm vào, bên cạnh đó, nó linh hoạt và rất nhanh.
     + Công cụ này cung cấp cho các nhà nghiên cứu và nhà tư vấn bảo mật khả năng cho thấy việc truy cập trái phép từ xa vào hệ thống sẽ dễ dàng như thế nào.
     + Cú pháp:

*[[[-l LOGIN|-L FILE] [-p PASS|-P FILE|-x OPT -y]] | [-C FILE]] [-e nsr] [-u] [-f|-F] [-*

*M FILE] [-o FILE] [-b FORMAT] [-t TASKS] [-T TASKS] [-w TIME] [-W TIME] [-m*

*OPTIONS] [-s PORT] [-c TIME] [-S] [-O] [-4|6] [-I] [-vV] [-d] server service [OPTIONS]*

|  |  |
| --- | --- |
| Tham số | Mô tả |
| Target | mục tiêu để tấn công, có thể là địa chỉ IPv4, địa chỉ IPv6 hoặc  tên DNS. |
| Service | một dịch vụ để tấn công, bao gồm danh sách các giao thức có  sẵn |
| -R | khôi phục một phiên bị hủy bỏ trước đó. |
| -S | kết nối qua SSL |
| -O | sử dụng SSL cũ v2 và v3 |
| -s port | nếu dịch vụ nằm trên một cổng mặc định khác, hãy xác định nó  ở đây |
| -l login | đăng nhập FILE với tên ĐĂNG NHẬP hoặc tải một số thông tin  đăng nhập từ FILE |
| -p pass | thử PASS mật khẩu hoặc tải một số mật khẩu từ FILE |
| -x min:max:charset | tạo mật khẩu từ độ dài tối thiểu đến tối đa. bộ ký tự có thể chứa 1 cho các số, a cho các ký tự viết thường và A cho các ký tự viết  hoa. Bất kỳ ký tự nào khác được thêm vào sẽ được đưa vào danh sách. |
| -y | vô hiệu hóa việc sử dụng các ký hiệu trong -x bruteforce |
| -e nsr | kiểm tra bổ sung, "n" cho mật khẩu rỗng, "s" thử đăng nhập  bằng mật khẩu, "r" thử đăng nhập ngược lại bằng mật khẩu |
| -C FILE | định dạng "đăng nhập: mật khẩu" được phân tách bằng dấu hai  chấm |
| -u | theo mặc định, Hydra kiểm tra tất cả mật khẩu cho một lần đăng  nhập và sau đó thử đăng nhập tiếp theo |
| -f | thoát sau cặp đăng nhập / mật khẩu được tìm thấy đầu tiên |
| -F | thoát sau cặp đăng nhập / mật khẩu được tìm thấy đầu tiên cho  bất kỳ máy chủ nào |
| -M FILE | danh sách máy chủ cho các cuộc tấn công song song, một mục  nhập trên mỗi dòng |
| -o FILE | ghi các cặp đăng nhập / mật khẩu được tìm thấy vào FILE thay  vì stdout |
| -b FORMAT | chỉ định định dạng cho -o FILE: text (mặc định), json, jsonv1 |
| -t TASKS | chạy TASKS số lượng kết nối song song |
| -m OPTIONS | tùy chọn mô-đun cụ thể |
| -w TIME | xác định thời gian chờ tối đa tính bằng giây cho các phản hồi |
| -W TIME | xác định thời gian chờ giữa mỗi kết nối mà một tác vụ thực  hiện. |

|  |  |
| --- | --- |
| -c TIME | thời gian chờ tính bằng giây cho mỗi lần đăng nhập trên tất cả  các luồng |
| -4/-6 | ưu tiên địa chỉ IPv4 (mặc định) hoặc IPv6 |
| -v / -V | chế độ chi tiết / hiển thị kết hợp đăng nhập + mật khẩu cho mỗi  lần thử |
| -d | Chế độ debug |
| -I | bỏ qua một file khôi phục hiện có |

* 1. **gawk**
     + Lệnh gawk trong Linux được sử dụng để quét và xử lý mẫu (pattern).
     + Lệnh awk không yêu cầu biên dịch và cho phép người dùng sử dụng các biến, hàm số, hàm chuỗi và toán tử logic.
     + Nó là một tiện ích cho phép các lập trình viên viết các chương trình nhỏ và hiệu quả dưới dạng các câu lệnh xác định các mẫu văn bản sẽ được tìm kiếm, trong một tài liệu văn bản và hành động sẽ được thực hiện khi tìm thấy một kết quả phù hợp trong một dòng.
     + Lệnh gawk có thể sử dụng để
       - Quét từng dòng một file.
       - Tách từng dòng đầu vào thành các trường.
       - Điều kiện và vòng lặp.
       - Phép toán số học và chuỗi.
       - Định dạng các dòng đầu ra.
       - Tạo báo cáo định dạng.
       - Chuyển đổi file dữ liệu.
       - Thực hiện (các) hành động trên các dòng phù hợp.
       - So sánh dòng / trường đầu vào với mẫu.
     + Cú pháp:

*gawk [POSIX / GNU style options] -f progfile [--] file ... gawk [POSIX / GNU style options] [--] 'program' file ...*

|  |  |
| --- | --- |
| Tùy chọn | Mô tả |
| -f progfile, –file=progfile | Đọc nguồn chương trình AWK từ tệp chương  trình tệp, thay vì từ đối số dòng lệnh đầu tiên. |
| -F fs, –field-separator=fs | Nó sử dụng FS cho bộ phân tách trường đầu vào  (giá trị của biến được xác định trước FS). |
| -v var=val, –assign=var=val: | Gán giá trị val cho biến var, trước khi bắt đầu  thực thi chương trình. |

# Nội dung thực hành

# Chuẩn bị môi trường

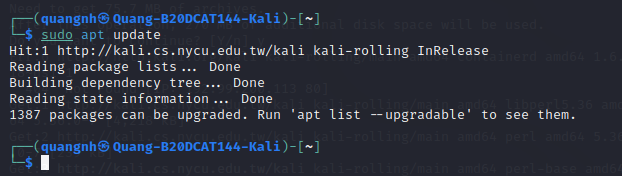
* + - Phần mềm VMWare Workstation.
    - Các file máy ảo VMWare và hệ thống mạng đã cài đặt: máy trạm, máy Kali Linux, máy chủ Windows và Linux.
    - Toppo mạng đã cấu hình.

# Các bước thực hành

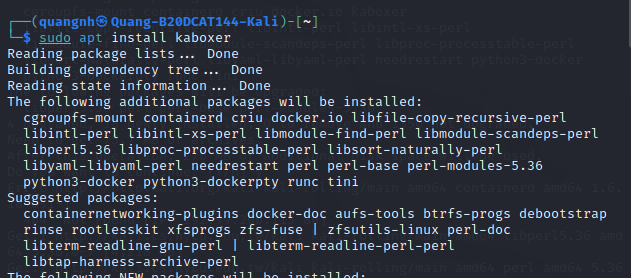
# Phân tích log sử dụng grep trong Linux

* + Cài đặt zenmap

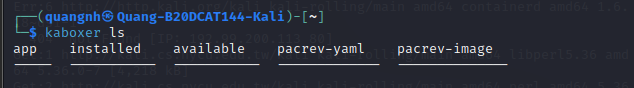
*sudo apt update*

**

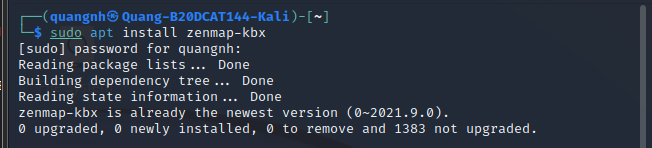
*sudo apt install kaboxer –y*



*kaboxer ls*

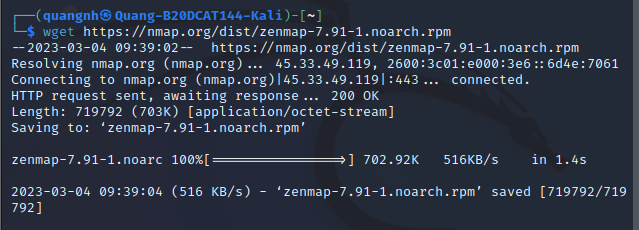
**

*sudo apt install zenmap-kbx*

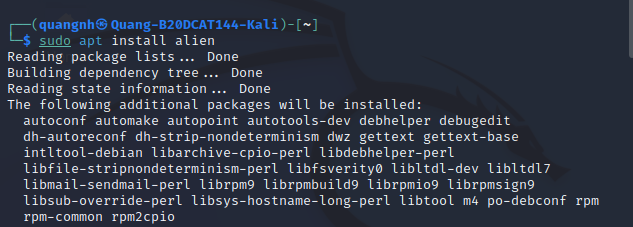
**

* Tải xuống zenmap từ trang chủ

*wget* [*https://nmap.org/dist/zenmap-7.91-1.noarch.rpm*](https://nmap.org/dist/zenmap-7.91-1.noarch.rpm)

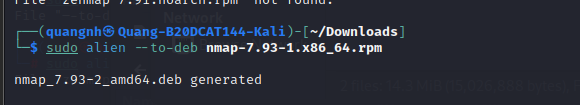
**

* + - Cài đặt alien package



* + - Chuyển đổi zenmap.rpm thành zenmap.deb bằng cách sử dụng alien

sudo alien --to-deb zenmap-7.91.noarch.rpm



# Tài liệu tham khảo

* 1. grep: <https://linuxcommand.org/lc3_man_pages/grep1.html>
  2. find: [https://docs.microsoft.com/en-us/windows-server/administration/windows- commands/find](https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/find)
  3. xhydra: <http://manpages.ubuntu.com/manpages/bionic/man1/hydra.1.html>
  4. gawk: [gawk command in Linux with Examples - GeeksforGeeks](https://www.geeksforgeeks.org/gawk-command-in-linux-with-examples/)
  5. [How to Install Zenmap in Kali Linux 2021.4 - TECH DHEE](https://techdhee.in/install-zenmap-in-kali-linux/?fbclid=IwAR0ZUewxVX8r5ujIqh8EzMH87yHAWSirrK3r17FoXdog7H_pQeQ1LGAh2I4)
  6. [How To Install the Apache Web Server on Ubuntu 20.04 | DigitalOcean](https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-ubuntu-20-04?fbclid=IwAR3k2iJckPCNzBnpRFKDyKQnKh7rcUge4VPX3MtfFJpYMktPqwQLH6bWafQ)