LAB 1 - TỔNG QUAN KALI LINUX

An toàn Mạng – NT140.P11.ANTN

Ngày báo cáo: 26/09/2024

GVHD: Nghi Hoàng Khoa

Tên nhóm: 5

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và Tên | MSSV | Nội dung công việc đã làm |
| 1 | Nguyễn Đức Luân | 22520825 | 3, 7, 8, 9 |
| 2 | Đào Hoàng Phúc | 22521110 | 13, 14, 15, 16 |
| 3 | Vũ Ngọc Quốc Khánh | 22520661 | 21, 22, 23, 24 |

A close up of a text

Description automatically generated

Câu 3:

-Sử dụng lệnh find ~ -type f -mtime 1 ! -user root -exec ls -l {} \;\n

A screen shot of a computer screen

Description automatically generated

A close-up of a text

Description automatically generated

Câu 7:

-Lịch sử các lệnh được lưu ở file có tên .zsh\_history ở thư mục home/user

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

-Các ưu nhược điểm khi thực hiện lưu trữ các lệnh đã nhập:

\*Ưu điểm:

+Mang tính tiện lợi vì cho phép truy cập nhanh chóng đến các lệnh đã sử dụng trước đó, đỡ mất thời gian để gõ lệnh, đặc biệt là các câu lệnh dài và phức tạp.

+Có thể tái thực thi các lệnh trước đó thông qua phím mũi tên lên và xuống hoặc sử dụng lệnh !<số thứ tự của lệnh đó trong history>

+Thuận tiện trong việc đánh giá, truy vết trong hệ thống khi có sự cố xảy ra, giúp kiểm tra lại các câu lệnh đã thực thi gây thay đổi trong hệ thống, từ đó đưa ra cách xử lý nhanh chóng.

\* Nhược điểm:

+Rủi ro bảo mật: Những thông tin nhạy cảm được nhập trong các câu lệnh có thể được lưu trữ trong file history, có nguy cơ trở thành rủi ro bảo mật nếu có người dùng không được cấp quyền truy cập được nhưng thông tin đó.

+Bị ghi đè, mất câu lệnh được lưu vì file history mặc định sẽ có kích thước giới hạn và các câu lệnh cũ sẽ có khả năng bị ghi đè nếu lượng lưu trữ vượt quá mức.

+Thiếu ngữ cảnh vì không biết câu lệnh đó được thực hiện trong biến môi trường hay thư mục nào, khiến việc sửa lỗi, khắc phục sự cố trở nên khó khăn hơn\

+Gây nhầm lẫn đối với các hệ thống nhiều người dùng khi các người dùng tại cùng một phiên thực hiện nhiều lệnh khác nhau khiến file history lưu tất cả các lệnh được sử dụng vào chung một file

Câu 8:

Có cách để thực hiện ngăn chạn việc lưu trữ lệnh bằng việc thực hiện các bước như sau:

B1: Sử dụng lệnh vim .zshrc để thay đổi nội dung file bash

B2:

+Comment lại các lệnh sau trong file bash:

HISTFILE=~/.bash\_history

HISTSIZE=1000

HISTFILESIZE=2000

+Thêm vào các lệnh sau vào file bash:

unset HISTFILE

export HISTSIZE=0

export HISTFILESIZE=0

Kết quả sau khi chỉnh sửa:

A screenshot of a computer

Description automatically generated

B3: chạy lại file bash bằng cách thực hiện lệnh sau:

source .zshrc

B4: Kiểm tra lại kết quả thực hiện:

A screenshot of a computer

Description automatically generated

Câu 9:

-Có thể sử dụng tổ hợp phím Ctrl+R để tìm lại các lệnh trước đó đã nhập:

A screenshot of a computer

Description automatically generated

Nếu đã tìm được lệnh muốn thực hiện chỉ cần nhấn ENTER để thực thi lệnh đó.

10. Như đã biết, khi sử dụng toán tử “>” để xuất kết quả vô tập tin, nếu tập tin đa tồn

tại, nội dung trong tập tin sẽ bị thay thế bằng nội dung mới. Vậy, có cách nào để

hoàn tác lại quá trình này hay không? Nếu có, hãy mô tả cách làm.

Không có cách nào để hoàn tác quá trình của tập tin bị ghi đè vì nội dung của tập tin cũ đã mất hoàn toàn và hệ thống không tự động sao lưu bản sao của tập tin cũ

13. Tải tập tin access\_log.txt.gz tại

(https://github.com/blakduk/ahihi/raw/master/access\_log.txt.gz), sau đó thực

hiện liệt kê danh sách các địa chỉ IP và số lượng tương ứng, thực hiện sắp xếp

giảm dần.

A screenshot of a computer

Description automatically generated

Figure 1: Tải về và giải nén tệp yêu cầu

Chạy lệnh này để liệt kê danh sách địa chỉ IP và số lượng tương ứng theo thứ tự giảm dần

**sort access\_log.txt | uniq -c | sort -nr**

A screen shot of a computer

Description automatically generated

Figure 2: Màn hình thực hiện lệnh

14. Hãy cho biết đường đẫn thực thi của 2 lệnh wget và curl?

A screenshot of a computer

Description automatically generated

Figure 3: Màn hình kiểm tra đường dẫn thực thi của 2 lệnh wget và curl

15. Theo bạn, trong 2 lệnh tải về wget và curl, lệnh nào ưu việt hơn? Giải thích?

Nhìn chung, nếu chỉ xét về tải về (Download) thì wget là lệnh ưu việt hơn   
Vì:

* Mặc định hỗ trợ tiếp tục tải các tệp bị gián đoạn mà không cần thêm tùy chọn phức tạp. Chỉ cần sử dụng tùy chọn **-c**, nó sẽ tự động kiểm tra và tiếp tục tải từ điểm dừng, ngay cả khi kết nối bị gián đoạn hoặc mất.
* Có khả năng tải toàn bộ website hoặc các thư mục với tất cả các tệp liên quan bằng cách sử dụng tùy chọn **-r** (recursive). Điều này rất hữu ích khi cần sao lưu hoặc tải nội dung trang web.
* Hỗ trợ tải xuống tệp từ một danh sách URL (trong một tệp văn bản) một cách dễ dàng. Chỉ cần tạo tệp chứa danh sách các URL và sử dụng lệnh
* Có tùy chọn **-b** giúp dễ dàng tải tệp về ở chế độ nền (background) mà không cần sử dụng thêm các công cụ của shell.

16. Có thể sử dụng lệnh curl để thay đổi các HTTP header được hay không? Nếu được,

cho ví dụ?

Có thể   
Ở đây gửi đi HTTP request với Header được thêm vào là Authorization Header : Bearer Token

A black background with green text

Description automatically generated

Figure 4: Màn hình thực hiện request HTTP POST tới local server API trả về danh sách các phim có trong database với quyền admin

21. Thực hiện lại chi tiết kịch bản Reverse Shell và Bind Shell sử dụng netcat.

Bind shell

A computer code with numbers and letters

Description automatically generated

A screen shot of a computer

Description automatically generated

Reverse shell

A computer screen shot of a computer code

Description automatically generated

A screenshot of a computer

Description automatically generated

22. So sánh ưu và nhược điểm khi sử dụng Reverse Shell và Bind Shell? Khi nào nên

sử dụng Bind Shell? Khi nào nên sử dụng Reverse Shell?

|  |  |  |
| --- | --- | --- |
| Tiêu chí | Bind Shell | Reverse Shell |
| Ưu điểm | Không cần attacker phải mở sẵn port | Dễ vượt qua tưởng lửa có rule Inbound |
| Nhược điểm | Khó vượt qua tường lửa có rule Inbound | Cần attacker mở sẵn port |
| Khi nào nên sử dụng | Khi tường lửa không có rule Inbound và cần linh động trong lúc attack | Khi tường lửa có rule Inbound |

23. Thực hiện trao đổi tập tin, bind shell và reverse shell sử dụng PowerShell

Trao đổi tập tin

A screenshot of a computer

Description automatically generated

Reverse Shell

A computer screen shot of a computer code

Description automatically generated

A screenshot of a computer

Description automatically generated

Bind Shell

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

24. Ngoài netcat và powershell, còn cách nào có thể tạo ra được reverse shell và bind

shell không? Cho một ví dụ.

Có rất nhiều cách để tạo shell như trang web [RevShell](https://www.revshells.com/) hoặc python reverse shell

Ví dụ về python reverse shell

A screenshot of a computer

Description automatically generated