BÁO CÁO THỰC HÀNH

**Môn học: An toàn mạng**

**Tên chủ đề: TỔNG QUAN KALI LINUX**

*GVHD: Tô Trọng Nghĩa*

1. **THÔNG TIN CHUNG:**

*Lớp: NT140.O11.ANTT*

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và tên | MSSV | Email |
| 1 | Nguyễn Đình Luân | 21521105 | 21521105@gm.uit.edu.vn |
| 2 | Trần Thanh Triều | 21522713 | 21522713@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Nội dung | Tình trạng |  |
| 1 | Yêu cầu bắt buộc | 100% | |
| 2 | Yêu cầu làm thêm | 85% | |
| Điểm tự đánh giá | | | **8.5/10** |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

1. Sử dụng lệnh which để xác định ví trị lưu trữ của lệnh pwd.

A screenshot of a computer

Description automatically generated

2. Sử dụng lệnh locate để xác định ví trí lưu trữ wce32.exe.

- Trước khi gõ lệnh locate wce32.exe, ta nên gõ lệnh updatedb trước.

A screen shot of a computer

Description automatically generated3. Sử dụng lệnh find để xác định bất kỳ tập tin (không phải thư mục) đã được sửa đổi vào ngày trước đó, KHÔNG thuộc sở hữu của user root và thực thi lệnh ls -l trên chúng. KHÔNG được sử dụng các lệnh pipeline/chaining

Ta sử dụng câu lệnh: find -type f ! -user root -mtime +1 -exec ls -l {} \;

Trong đó:

* type f !: chỉ tìm kiếm tập tin
* ! -user root loại trừ các tập tin
* -mtime +1: chỉ các tập tin đã được sửa đổi trước đó (trước ngày hiện tại) sẽ được tìm kiếm.
* -exec ls -l {} \;: Sử dụng ls -l để hiển thị thông tin chi tiết về các tập tin tìm thấy.

A computer screen shot of a program

Description automatically generated

4. Liệt kê các port đang được mở trên Kali Linux

A screen shot of a computer

Description automatically generated

5. Tại sao khi kiểm tra dịch vụ SSH có đang chạy hay không (Hình 10), kết quả hiển thị 2 dòng, trong khi dịch vụ HTTP (Hình 13), kết quả chỉ có 1 dòng

SSH là một hệ thống xác thực tên người dùng / mật khẩu tích hợp để thiết lập kết nối. Việc trao đổi thông tin giữa Client-Server cần phải có sự kết nối qua lại giữa 2 thực thể, vì thế SSH sẽ cần 2 cổng để có thể giao tiếp với nhau. Trong khi đó, HTTP có nghĩa là giao thức truyền siêu văn bản. Giao thức này xác định cách các thông báo được định dạng và truyền đi nên không cần tới 2 cổng để giao tiếp.

6.Ngăn dịch vụ SSH chạy cùng với hệ thống lúc khởi động dùng câu lệnh:

sudo systemctl disable ssh

A screen shot of a computer

Description automatically generated

7. Lịch sử các lệnh thực ra được lưu trữ ở đâu? Liệt kê các ưu, nhược điểm khi thực hiện lưu trữ lại các lệnh đã nhập?

- Lịch sử các lệnh thực ra được lưu trữ ở .bash\_history. Ưu điểm khi thực hiện lưu trữ lại các lệnh là với việc lưu trữ trước các lệnh thì việc có thể xem lại một lệnh ta đã quên trước đó có thể thực hiện nhanh chóng và tiện lợi. Nhược điểm là việc lưu trữ các lệnh đã nhập sẽ bao gồm những câu lệnh sai trước đó, khiến ta dễ bị nhầm lẫn giữa các lệnh khác với nhau.

8. Có cách nào để ngăn chặn việc lưu trữ lịch sử lệnh hay không? Nếu có, hãy mô tả cách làm.

Dùng lệnh export HISTSIZE=0

A computer screen shot of a computer code

Description automatically generated

9. Ngoài cách sử dụng tiện ích history expansion, còn cách nào để thực hiện lại các lệnh đã nhập một cách nhanh chóng hay không? Nếu có, hãy mô tả cách làm.

Ngoài sử dụng tiện ích history expansion, ta có thể dùng phím control của keyboard: nút lên và nút xuống. Với nút lên, ta có thể dễ dàng lấy được các câu lệnh đã thực thi, nhấn càng nhiều thì câu lệnh càng xa phía trên được phục hồi. Trong khi đó, phím nút xuống sẽ ngược lại.

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

Hầu như các tác vụ được thực hiện trong Linux không thể undo các chức năng mà ta đã thực hiện. Để có thể tránh những sự kiện đáng tiếc, ta nên xem xét tạo ra một file backup trước khi thực hiện nó với tập tin chính. Hoặc là sử dụng toán tử “>>” để có thể giữ lại cả cái cũ và mới, sau đó xem xét nên chọn hay loại cái nào.

11. Sử dụng lệnh cat cùng với lệnh sort để sắp xếp lại nội dung của tập tin /etc/passwd, sau đó lưu kết quả vào một tập tin mới có tên passwd\_new và thực hiện đến số lượng dòng có trong tập tin mới

dùng lệnh **cat /etc/passwd | sort > passwd\_new** để sắp xếp lại nội dung của tệp passwd và lưu vào file paswd\_new sau đó dùng lệnh **echo "Số lượng dòng trong tệp passwd\_new: $(wc -l < passwd\_new)"** để in ra thông báo số dòng của passwd\_new

A screen shot of a computer

Description automatically generated

12. Sử dụng tập tin /etc/passwd, trích xuất tên user và home directory cho tất cả user có shell được thiết lập là /usr/sbin/nologin. Lưu ý, chỉ sử dụng 1 dòng lệnh duy nhất. Kết quả xuất ra màn hình như hình dưới

Lệnh này sử dụng tệp /etc/passwd làm nguồn dữ liệu, sử dụng dấu hai chấm làm phân tách giữa các trường trong tệp /etc/passwd. Sau đó tìm kiếm các dòng trong tệp /etc/passwd mà có shell được thiết lập là /usr/sbin/nologin và in ra như trong hình

A screen shot of a computer

Description automatically generated

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.

Tải về và giải nén:

A computer screen shot of a computer code

Description automatically generated

Sử dụng câu lệnh: **cat access\_log.txt | awk '{print $1}' | sort | uniq -c | sort -rn | awk '{print "The IP address " $2 " has hit " $1 " times"}'**

cat access\_log.txt: Sử dụng cat để đọc nội dung của tệp log access\_log.txt.

awk '{print $1}': Sử dụng awk để trích xuất trường đầu tiên (địa chỉ IP) từ mỗi dòng trong tệp log. Đây là phần tử '{print $1}'.

sort: Sử dụng sort để sắp xếp danh sách các địa chỉ IP.

uniq -c: Sử dụng uniq -c để đếm số lần xuất hiện của mỗi địa chỉ IP và thêm số đếm vào trước địa chỉ IP.

sort -rn: Sử dụng sort -rn để sắp xếp danh sách theo số lần xuất hiện giảm dần.

awk '{print "The IP address " $2 " has hit " $1 " times"}': Sử dụng awk lần nữa để tạo thông điệp cho mỗi dòng kết quả. Đây là phần tử '{print "The IP address " $2 " has hit " $1 " times"}'. Câu lệnh sẽ kết hợp địa chỉ IP và số lần xuất hiện vào một chuỗi thông điệp theo cú pháp "The IP address [địa chỉ IP] has hit [số lần] times."

A screen shot of a computer

Description automatically generated

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

Sử dụng which để lấy đường dẫn thực thi của 2 câu lệnh

A screen shot of a computer program

Description automatically generated

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

Lệnh curl vượt trội hơn vì:

- hỗ trợ nhiều giao thức hơn như HTTP, FTP, SCP, SFTP, IMAP, SMTP, và nhiều giao thức khác.

- có khả năng thực hiện các yêu cầu HTTP, gửi dữ liệu biểu mẫu, xử lý cookie, và thậm chí là xem nội dung trang web trực tiếp.

- có khả năng giao tiếp trực tiếp với các dịch vụ web, gửi yêu cầu RESTful API, hoặc thực hiện các tác vụ phức tạp hơn

16: Có thể sử dụng lệnh curl để thay đổi các HTTP header được hay không? Nếu được, cho ví dụ?

Có thể sử dụng lệnh curl để thay đổi các HTTP header khi gửi yêu cầu HTTP Ví dụ:

Sử dụng câu lệnh **curl -v -H "Custom-Header: MyCustomValue" https://example.com** trong đó option -H dùng để thay đổi HTTP header, option -v để hiển thị thông tin chi tiết về quá trình gửi và nhận dữ liệu qua giao thức HTTP

A screenshot of a computer program

Description automatically generated

Triển Khai ứng dụng chat:

A screenshot of a computer

Description automatically generated

A computer screen shot of a computer

Description automatically generated

17. Máy chủ nào sẽ đóng vai trò là server?

Máy chủ bên windows 10 sẽ đóng vai trò là server. Vì máy chủ windows 10 là nơi mở

port kết nối với các client.

18. Máy chủ nào sẽ đóng vai trò là client?

Máy chủ bên Kali sẽ đóng vai trò là client. Vì máy chủ kali là nơi chủ động kết nối

với IP của máy chủ tại cổng 4444.

19. Nếu khai báo lệnh “nc -lvnp 4444” thì thật chất, port 4444 được mở ở máy nào?

- Port 4444 sẽ được mở ở ngay tại máy chủ (Server)

20. Thực hiện chuyển tập tin wget.exe trên máy Kali sang máy Windows 10

A black background with white text

Description automatically generated

A screen shot of a computer

Description automatically generated

Kiểm tra tệp nhận được:

A screen shot of a computer screen

Description automatically generated

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

Bind Shell:

A black screen with white text

Description automatically generated

kết nối và chạy thử lệnh ipconfig

A computer screen shot of a computer

Description automatically generated

Reverse Shell:

Kết nối và chạy thử lệnh ipconfig

A computer screen shot 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?

- Ưu điểm khi sử dụng Reverse Shell là ta không cần phải tìm địa chỉ IP để kết nối trực

tiếp với host ở bên kia. Ta chỉ cần mở một trong những cổng thông dụng nhất để thu

kết nối từ host và chiếm dụng quyền điều khiển từ xa.

- Nhược điểm khi sử dụng Reverse Shell là ta luôn ở vị trí bị động và cổng mở có thể sẽ

không bao giờ được kết nối với host.

- Ưu điểm khi sử dụng Bind Shell là ta có thể điều khiển từ xa được Host ở bên kia

thông qua cổng port kết nối và địa chỉ IP của host.

- Nhược điểm khi sử dụng Bind Shell là ta sẽ phải mất một thời gian để tìm ra được

địa chỉ private của host bên kia và cổng kết nối mà host kia đang mở

23. Nhóm em chưa làm được

24. Chúng ta có thể sử dụng các ngôn ngữ lập trình như python, … để tạo bind shell và reverse shell

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)