BÁO CÁO THỰC HÀNH

**Môn học: An toàn mạng**

**Tên chủ đề: Tổng quan Kali Linux**

*GVHD: Tô Trọng Nghĩa*

**Nhóm: 21**

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: XXX

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và tên | MSSV | Email |
| 01 | Lê Đoàn Trà My | 21521149 | [21521149@gm.uit.edu.vn](mailto:21521149@gm.uit.edu.vn) |
| 02 | Nguyễn Thị Thanh Mai | 21521112 | [21521112@gm.uit.edu.vn](mailto:21521112@gm.uit.edu.vn) |

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

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Nội dung | Tình trạng | Trang |
| 1 | Tổng quan Kali Linux (Câu 1 – Câu 3) | 100% | 02 |
| 2 | Quản lý các dịch vụ (Câu 4 – Câu 6) | 100% | 03 - 04 |
| 3 | Command line (Câu 7 – Câu 16) | 100% | 04 - 10 |
| 4 | Các công cụ cần thiết (Câu 17 – Câu 24) | 100% | 10 – 18 |
| Điểm tự đánh giá | | | **9.5-10/10** |

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

BÁO CÁO CHI TIẾT

## Tổng quan Kali Linux

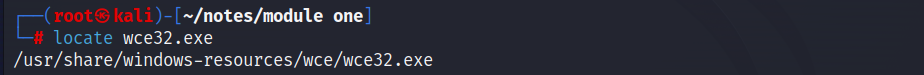


→ Trả lời:





→ Trả lời:



A close up of text

Description automatically generated

→ Trả lời: sử dụng lệnh **sudo find . -type f -mtime 1 ! -user root -ls**

Trong đó:

+ sudo find . : tìm file trong thư mục hiện tại với quyền root.

+ -type f : tìm tập tin.

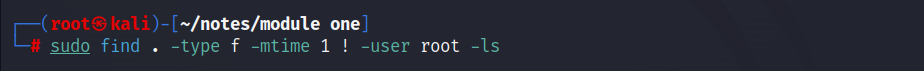
+ -mtime 1 : tập tin đã được sửa đổi vào ngày trước.

+ ! -user root: không thuộc sở hữu của user root.

+ -ls : tập tin trong một định dạng danh sách dài. Khi định dạng danh sách dài được sử dụng, bạn có thể thấy thông tin tệp sau: Loại tệp, Quyền đối với tệp, Số lượng liên kết cứng đến tệp, Chủ sở hữu tệp, Nhóm tệp, Kích thước tập tin, Ngày và giờ, Tên tệp.

+ -ls tương đương với cụm ls -dils.

Thử thực thi, kết quả thu được là không có tập tin nào đủ các điều kiện theo đề bài.



1. **Quản lý các dịch vụ**

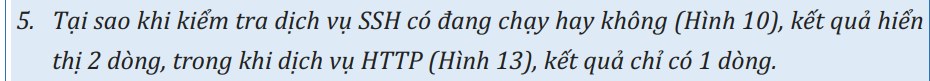
****

→ Trả lời: Có 3 port đang mở là 22, 80 và 43933.

Có thể xem bằng cách thử 3 câu lệnh

A screenshot of a computer

Description automatically generated

****

→ Trả lời: Xem xét kết quả khi kiểm tra dịch vụ SSH và HTTP

A computer screen with white text

Description automatically generated

A computer screen shot of a math equation

Description automatically generated

Giải thích: - Ở hình đầu tiên, dịch vụ SSH dựa trên giao thức TCP sẽ hỗ trợ IPv4 (dòng 1) và IPv6 (dòng 2) nên khi kiểm tra kết quả hiển thị 2 dòng.

- Ở hình thứ hai, dịch vụ HTTP không hỗ trợ IPv6.

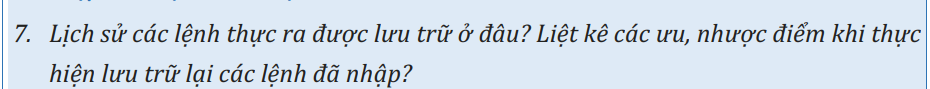
****

→ Trả lời: sử dụng lệnh **sudo systemctl disable ssh**

**A screen shot of a computer

Description automatically generated**

1. **Command line**

****

→ Trả lời: Lịch sử các lệnh được lưu trữ trong file **.zsh\_history**. Ngoài ra khi gõ trong terminal **history** cũng sẽ hiển thị các lệnh đã gõ.

A screenshot of a computer screen

Description automatically generated

- Xem nội dung trong file:

A screenshot of a computer program

Description automatically generated A screenshot of a computer program

Description automatically generated

- Nhận xét:

+ Ưu điểm:

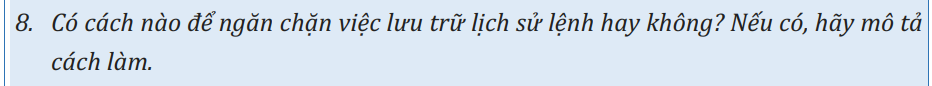
++ Lưu trữ tất cả các lệnh đã nhập từ lúc cài máy ảo Linux.

++ Dễ dàng truy xuất lại khi cần.

+ Nhược điểm:

++ Khi lưu trữ càng nhiều lệnh sẽ tiêu tốn tài nguyên.

++ Sẽ dễ bị lộ thông tin khi người khác truy cập trên máy tính.

****

→ Trả lời:

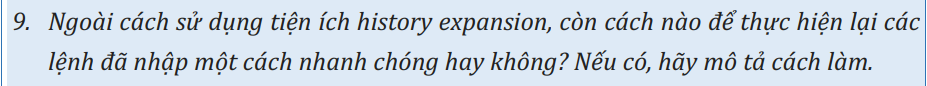
- Nếu lịch sử lệnh lưu trong file .bash\_history thì ta dùng lệnh set +o history sẽ ngăn cản

được việc lưu trữ lệnh. Và dùng lệnh set -o history để bật lại chế độ lưu trữ lệnh.

- Nh sử lệnh lưu trong file .zsh\_history thì ta gán **HISTSIZE=0**. Khi đó hệ thống chỉ lưu lại 1 lệnh duy nhất (lệnh mới vừa thực hiện). Tuy nhiên nó chỉ có tác động đến phiên làm việc hiện tại và tương lai. Lịch sử lệnh trong các phiên trước đó đã được lưu trong tệp tin lịch sử lệnh và không bị ảnh hưởng hay thay đổi gì.

A black background with white text

Description automatically generated with medium confidence

****

→ Trả lời:

- Để thực hiện lại các lệnh đã nhập 1 cách nhanh chóng ta có thể sử dụng phím mũi tên ⬆⬇ để xem lại lệnh đã nhập.

- Sử dụng phím tắt Ctrl + r sau đó nhập những kí tự đầu, chương trình sẽ gợi ý lệnh đã

dùng gần nhất.

**A close up of text

Description automatically generated**

→ Trả lời: Theo như nhóm em tìm hiểu thì hiện không có cách trực tiếp để hoàn tác lại quá trình này.

Tuy nhiên, nếu chỉ muốn khôi phục lại nội dung trước đó thì có thể sử dụng:

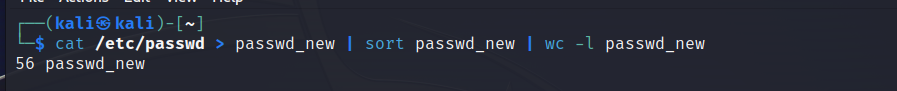
+ Sao lưu tập tin: tạo một bản sao lưu (backup) của tập tin trước khi ghi đè lên, có thể khôi phục lại nội dung ban đầu từ bản sao lưu đó.

+ Hệ thống quản lý phiên bản: Sử dụng hệ thống quản lý phiên bản như Git, có thể dùng nó để khôi phục lại phiên bản trước đó của tập tin.

**A close up of words

Description automatically generated**

→ Trả lời: **cat /etc/passwd > passwd\_new | sort passwd\_new | wc -l passwd\_new**

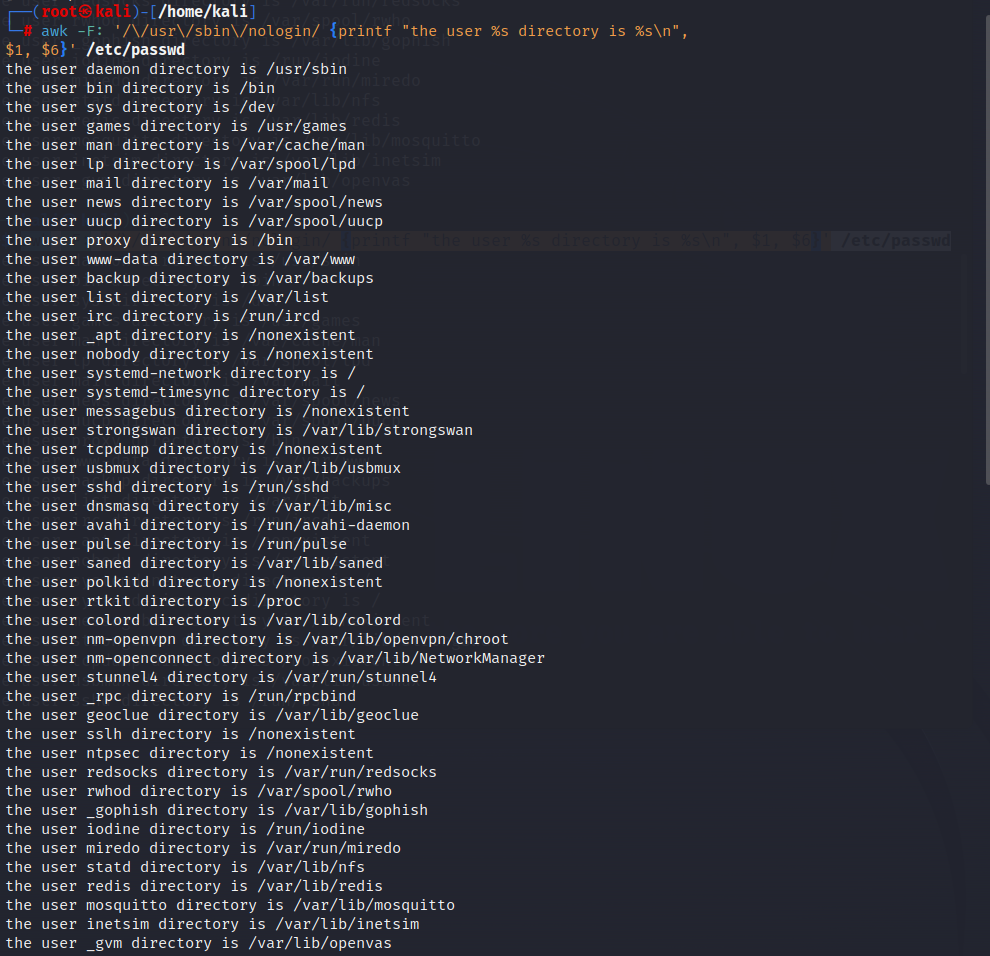


Đầu tiên cat tập tin passwd sau đó lưu kết quả tập tin vào passwd\_new bằng toán tử “>”. Sử dụng toán tử “|” để chuyển hướng kết quả của lệnh cat thành tham số đầu vào của lệnh sort. Sau đó tiếp tục sử dụng toán tử “|”để chuyển hướng kết quả của lệnh sort thành tham số đầu vào của lệnh wc

**A close up of words

Description automatically generated**

→ Trả lời: Sử dụng câu lệnh **awk -F: '/\/usr\/sbin\/nologin/ {printf "the user %s directory is %s\n", $1, $6}' /etc/passwd**

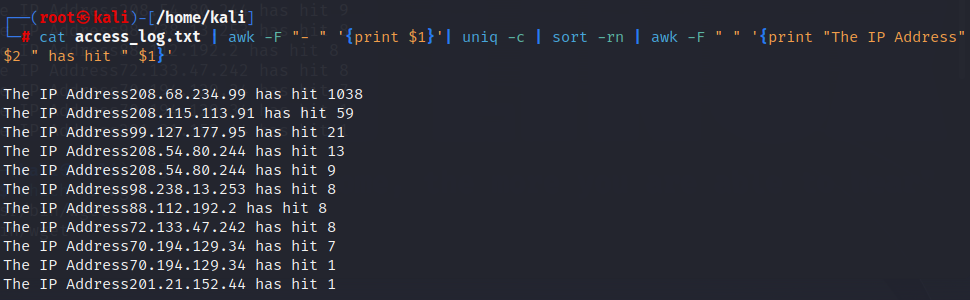
****

- $1, $6: trường thứ nhất là tên người dùng và trường thứ sáu là thư mục gốc (home directory).

**A close up of text

Description automatically generated**

→ Trả lời: Sử dụng lệnh **cat access\_log.txt | awk -F "- " '{print $1}'| uniq -c | sort -rn | awk -F " " '{print "The IP Address" $2 " has hit " $1}'**

****

- cat access\_log.txt để xem những đặc điểm của file.

- awk để xuất ra danh sách các IP.

- uniq -c: Lệnh uniq với tùy chọn -c để xuất ra màn hình số lần lặp của IP ở đầu dòng và

những IP lặp chỉ xuất hiện 1 lần.

- sort -rn: sắp xếp IP với số lần xuất hiện từ lớn đến nhỏ theo chữ số.

- lệnh awk thứ 2 để xuất ra màn hình theo yêu cầu đề bài với $2 là số lần xuất hiện của IP, $1 là IP.

****

→ Trả lời: Để tìm đường dẫn của một lệnh ta sử dụng lệnh which với option -a để biết những đường dẫn bị ẩn.

A black background with white text

Description automatically generated

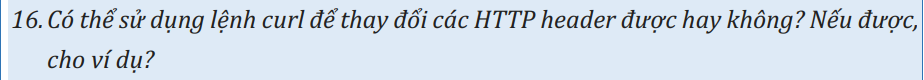
****

→ Trả lời: Nếu nhìn về tổng thể lệnh curl ưu việt hơn.

- Wget: Chương trình đơn giản, độc lập, tải xuống file nhanh chóng. Xử lý các tác vụ giống như trình duyệt, không cần cấu hình phức tạp. Cho phép tải xuống từ trang web hoặc thư mục FTP.

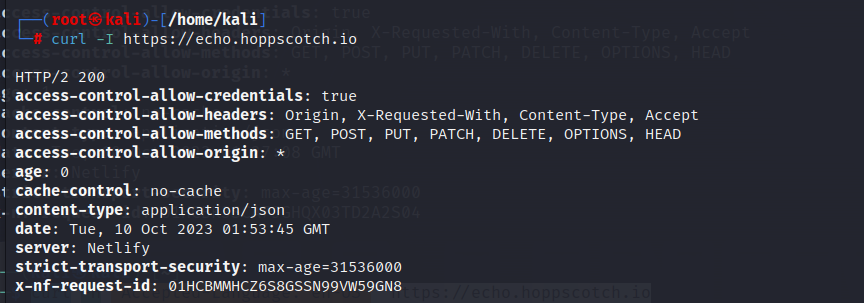
- Curl: Công cụ đa năng với sức mạnh của thư viện libcurl. Truy cập web qua HTTP, HTTPS, xử lý FTP và hỗ trợ LDAP, chia sẻ Samba, sử dụng cURL để gửi và nhận email. Có tính năng bảo mật, hỗ trợ SSL/TLS, proxy bao gồm SOCKS và nén gzip. - Được cập nhật, phát triển thường xuyên hơn so với “wget”

→ Nếu muốn tải xuống nhanh chóng mà không cần phải bận tâm về các flag, nên sử dụng wget - công cụ này vô cùng đơn giản. Nếu cần thực hiện một nhiệm vụ phức tạp hơn, cURL sẽ là lựa chọn đáng xem xét.

****

→ Trả lời: Có thể sử dụng lệnh curl để thay đổi các HTTP header.

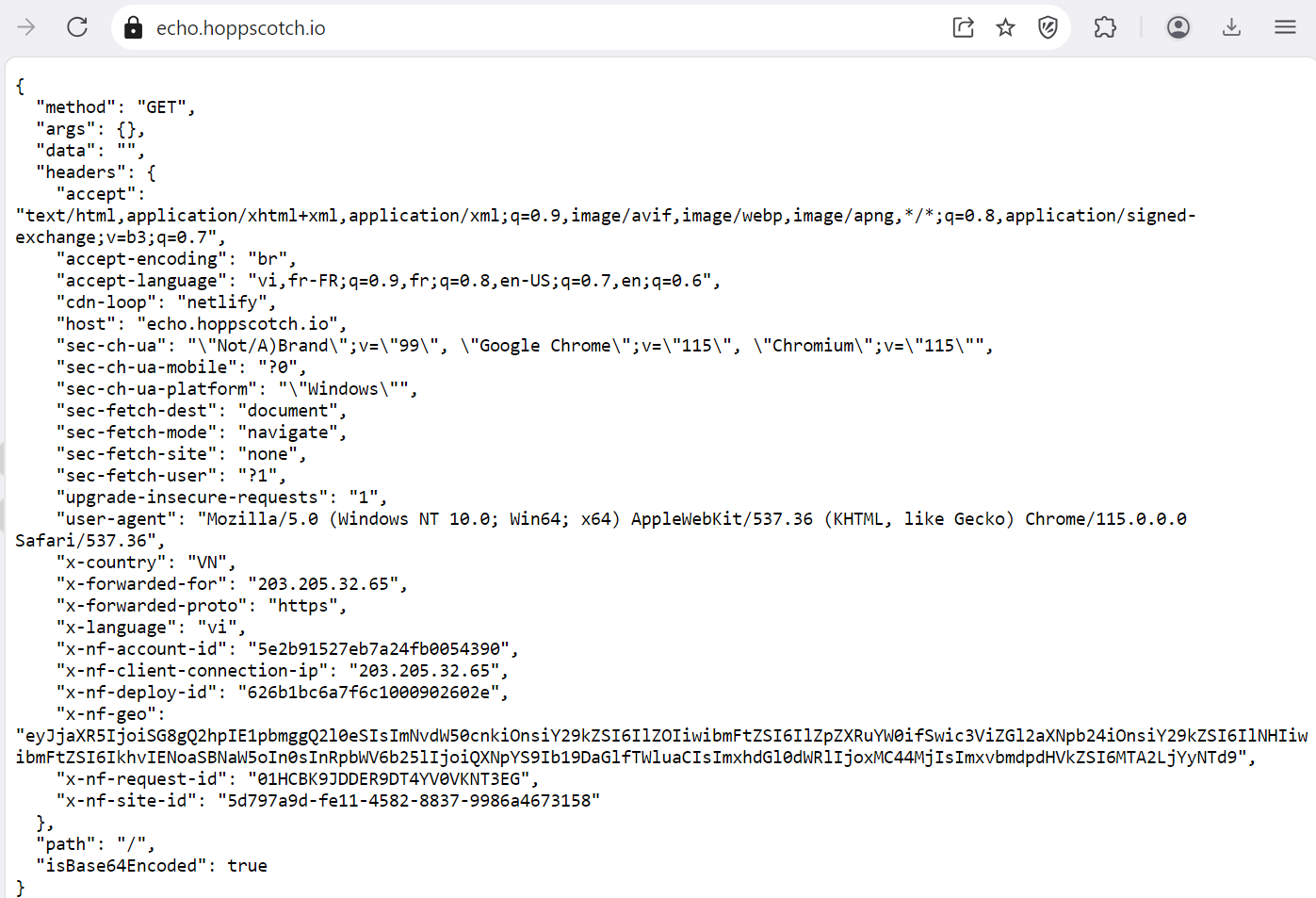
- Option -I để hiển thông tin HTTP Header.



- Option -H để có thể thiết lập các thông tin cho phần header của gói tin HTTP.

Cú pháp**: curl -H ‘Header: Value’ https://.....**

+ Nội dung khi truy cập bằng Cốc Cốc:

****

+ Kết quả khi thực hiện ví dụ với option -H:

**A computer screen shot of a computer code

Description automatically generated**

1. **Các công cụ cần thiết**

\* Triển khai ứng dụng chat đơn giản trên 2 máy Kali và Windowns 10. Trả lời các câu hỏi:

****

→ Trả lời: Máy Kali Linux.

****

→ Trả lời: Máy Windown 10.

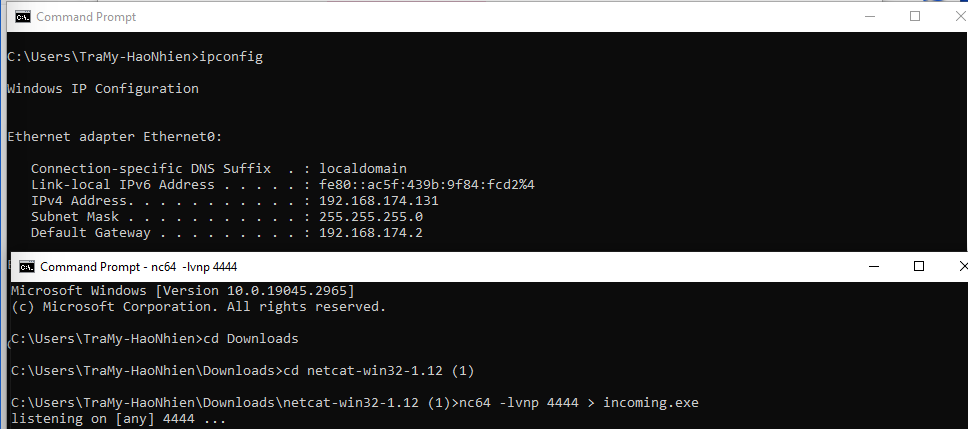
****

→ Trả lời: Port sẽ được mở ở máy thực hiện câu lệnh đó.

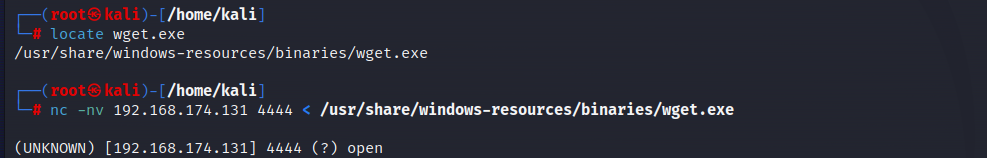
****

→ Trả lời:

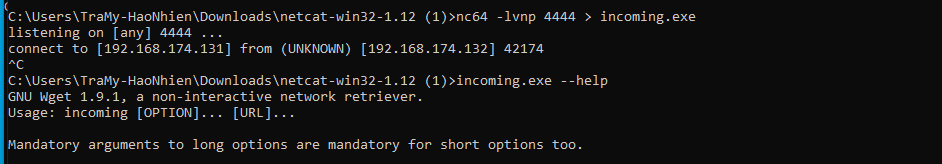
- Xem địa chỉ IP của máy Windows 10 và khai báo “nc -lvnp 4444”:

****

- Trên máy Kali, xác định đường dẫn của wget.exe và kết nối với máy Windows 10:



- Kết nối thành công và kiểm tra lại trong file incoming.exe:

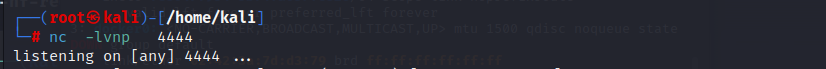


****

→ Trả lời:

**\* Reverse Shell:**

- Khai báo “nc -lvnp 4444” trên máy Kali:



- Windows 10 kết nối với Kali và cung cấp cmd cho Kali:



- Sau khi kết nối thành công, thực hiện 1 lệnh đơn giản trên cmd của Windows 10 được cung cấp cho Kali (ipconfig):

A screenshot of a computer

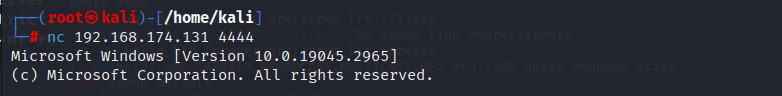
Description automatically generated

**\* Bind Shell:**

- Khai báo “nc -lvnp 4444” trên máy Windows 10:



- Kali kết nối với Windows 10:



- Thông tin kết nối trên Windows 10:

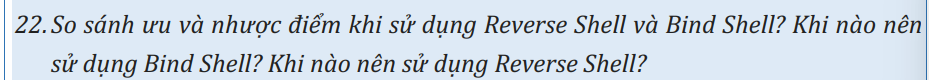
A screen shot of a computer

Description automatically generated

- Sau khi kết nối thành công, thực hiện 1 lệnh đơn giản trên cmd của Windows 10 được cung cấp cho Kali (ipconfig):

A screen shot of a computer

Description automatically generated

****

→ Trả lời:

|  |  |  |
| --- | --- | --- |
|  | Reverse Shell | Bind Shell |
| Ưu điểm | - Có thể vượt qua các vấn đề về tường lửa firewall.  - Không cần biết đến địa chỉ IP để truy cập máy tính.  - Thường là cách duy nhất để thực hiện quản lý từ xa tới host thông qua NAT. | - Có trình lắng nghe đang chạy trên mục tiêu. |
| Nhược điểm | - Hầu hết bất kỳ kết nối reverse shell nào cũng có thể là độc hại (trừ trường hợp cố tình sử dụng để quản trị từ xa).  - Không có cách nào chắc chắn để chặn các kết nối reverse shell trên hệ thống mạng. | - Khó vượt qua tường lửa firewall và NAT → Đôi khi Bind Shell không thành công.  - Phải biết địa chỉ IP và cổng để truy cập máy tính mục tiêu. |
| Sử dụng khi | - Không thể truy cập trực tiếp (không có IP public hoặc được bảo vệ bằng firewall, NAT).  - Thực hiện kiểm tra bảo mật (pentesting)/quản lý từ xa hợp pháp và có sự cho phép. | - Có quyền truy cập gốc (root) trên máy tính mục tiêu và tạo một liên kết lắng nghe trên máy tính đó.  - Trong các tình huống pentesting hoặc trong môi trường có sự cho phép và hợp pháp. |

****

→ Trả lời: Mở PowerShell với quyền Administrator: Mở Task Manage → Chọn File → Run new task → Xuất hiện hộp thoại Create new task, gõ powershell và chọn Create this task with administrative provileges → OK.

A screenshot of a computer

Description automatically generated

**\* Chuyển tập tin:**

- Tạo tập tin trên Kali:

A screen shot of a computer

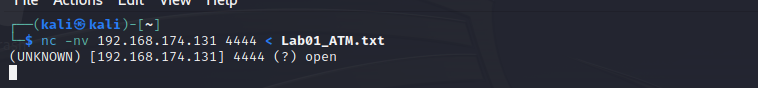
Description automatically generated

- Khai báo “nc -lvnp 4444” trên powershell Windows 10:

A screenshot of a computer screen

Description automatically generated

- Trên máy Kali, tiến hành kết nối và gửi file Lab1\_ATM.txt:



- Kết nối thành công và kiểm tra lại trong file coming.txt:

A screenshot of a computer screen

Description automatically generated

**\* Bind Shell:**

- Khai báo “nc -lvnp 4444” trên powershell Windows 10 và thông tin hiển thị sau khi Kali kết nối:

A blue screen with white text

Description automatically generated

- Kali kết nối và chiếm quyền:

A screenshot of a computer

Description automatically generated

**\* Reverse Shell:**

- Khai báo “nc -lvnp 4444” trên máy Kali:



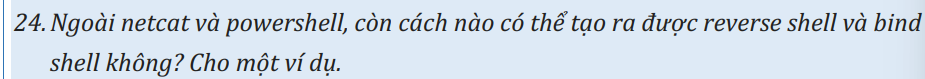
- Windows 10 kết nối Kali và cung cấp powershell:



- Sau khi kết nối thành công, thực hiện lệnh ipconfig để thử

A screenshot of a computer

Description automatically generated

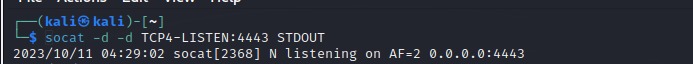
****

→ Trả lời: Có thể sử dụng một số ngôn ngữ lập trình: Python, Perl,… với module Socket tương ứng của ngôn ngữ; sử dụng Socat,…vv…

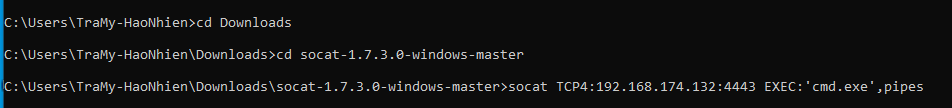
Chúng em sẽ thực hiện ví dụ tạo reverse shell và bind shell bằng socat.

**\* Reverse Shell:**

- Khai báo trên máy Kali:

****

- Windows 10 kết nối với Kali và cung cấp cmd cho Kali:



- Sau khi kết nối thành công, thực hiện lệnh ipconfig để thử trên Kali:

**A screenshot of a computer

Description automatically generated**

**\* Bind Shell:**

- Khai báo trên Windows10 và cho Kali kết nối thì màn hình Windows10:

**A computer screen shot of a program

Description automatically generated**

- Kali kết nối và chiếm quyền, thử thực hiện ipconfig:

**A computer screen shot of a computer program

Description automatically generated**

**- HẾT -**

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