BÁO CÁO THỰC HÀNH

**Bài thực hành số xx: Tên bài thực hành**

**Môn học:** Nhập môn Mạng máy tính

**Lớp:** NT100.ATTT.2

**THÀNH VIÊN THỰC HIỆN (Nhóm xx):**

|  |  |  |
| --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** |
| 1 | Nguyễn Thị A | 20520001 |
| 2 | Phan Văn B | 20520002 |
|  |  |  |

|  |
| --- |
| **Điểm tự đánh giá** |
|  |

**ĐÁNH GIÁ KHÁC:**

|  |  |
| --- | --- |
| Tổng thời gian thực hiện |  |
| Phân chia công việc |  |
| Ý kiến *(nếu có)*  + Khó khăn  + Đề xuất, kiến nghị |  |

Phần bên dưới của báo cáo này là báo cáo chi tiết của nhóm thực hiện

MỤC LỤC

[**A.** BÁO CÁO CHI TIẾT 2](#_Toc110261086)

[1. Tổng quan kali linux 2](#_Toc110261087)

[a. Các lệnh linux cơ bản 2](#_Toc110261088)

[b. Tìm kiếm trong kali linux 3](#_Toc110261089)

[2. Nội dung 2 3](#_Toc110261090)

[a. Nội dung a 3](#_Toc110261091)

[**B.** TÀI LIỆU THAM KHẢO 3](#_Toc110261092)

# BÁO CÁO CHI TIẾT

## Tổng quan kali linux

### Các lệnh linux cơ bản

* Bài thực hành 1: Liệt kê các tập tin

Ảnh có chứa văn bản

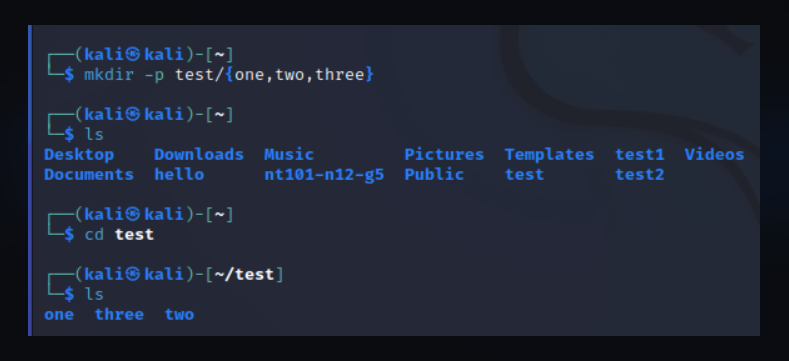
Mô tả được tạo tự động

* Bài thực hành 2: Di chuyển xung quanh

Ảnh có chứa văn bản, màn hình, tường, thiết bị điện tử

Mô tả được tạo tự động

* Bài thực hành 3: Tạo thư mục



### Tìm kiếm trong Kali Linux

* **Bài thực hành 4: which**

Ảnh có chứa văn bản

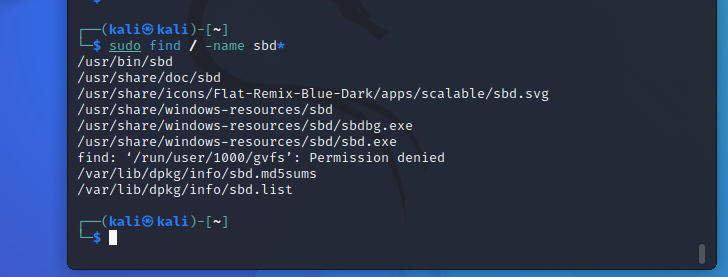
Mô tả được tạo tự động

* Bài thực hành 5: locate

Ảnh có chứa văn bản

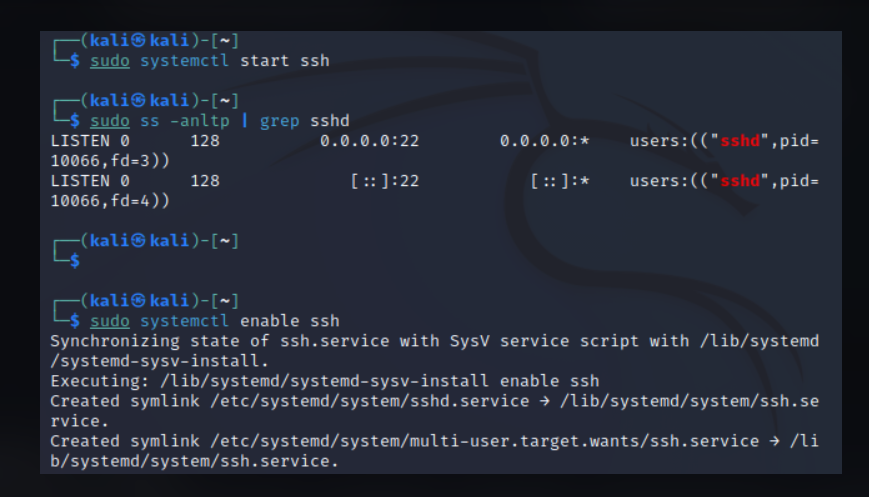
Mô tả được tạo tự động

* Bài thực hành 6: find



## Quản lý các dịch vụ

* Bài thực hành 6: Dịch vụ SSH



* Bài thực hành 7: Dịch vụ HTTP

Ảnh có chứa văn bản

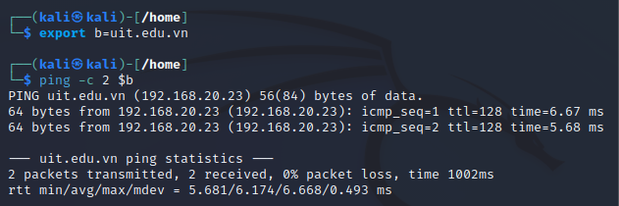
Mô tả được tạo tự động

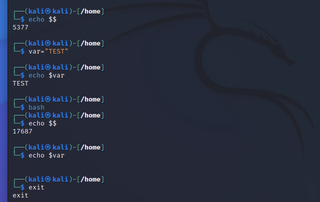
## Command line

### Bash environment

* Bài thực hành 8: biến môi trường

### Không có mô tả.

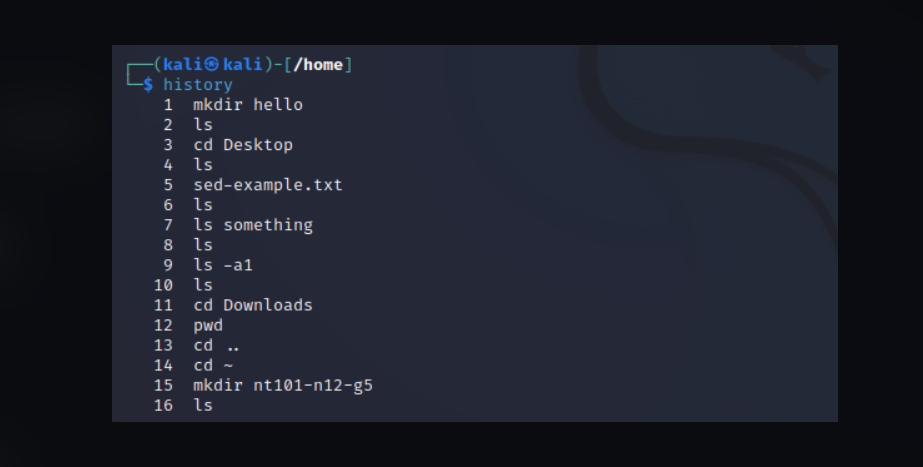




Ảnh có chứa văn bản

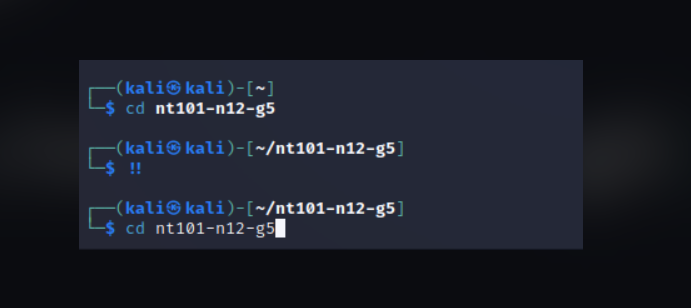
Mô tả được tạo tự động

* Bài thực hành 9: bash history



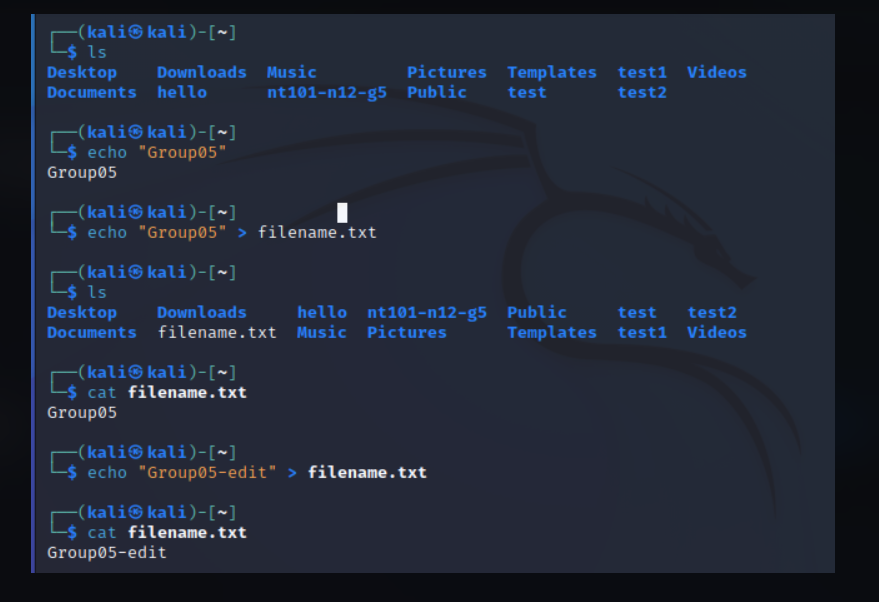
Ảnh có chứa văn bản, màn hình, đặt, tối

Mô tả được tạo tự động



### Piping và chuyển hướng

* Bài thực hành 10: Chuyển hướng đến các tập tin mới



* Bài thực hành 11: chuyển hướng đến tập tin đã tồn tại

Ảnh có chứa văn bản, màn hình, tường, TV

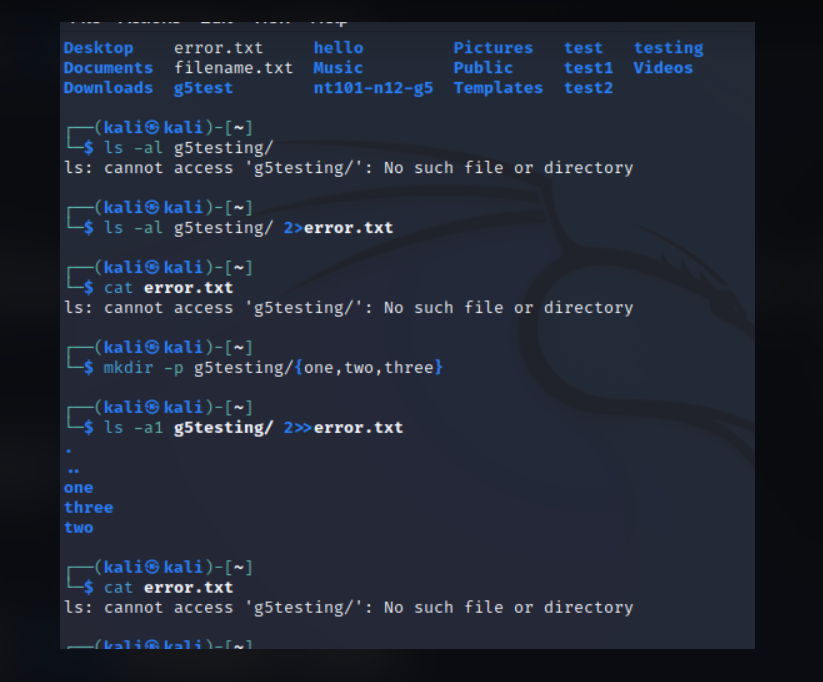
Mô tả được tạo tự động

* Bài thực hành 12: Chuyển hướng từ một tập tin

Ảnh có chứa văn bản, màn hình, tối, đặt

Mô tả được tạo tự động

* Bài thực hành 13: Chuyển hướng STDERR



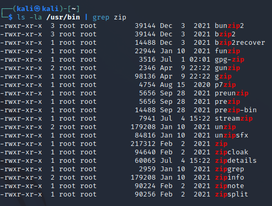
* Bài thực hành 14: Piping

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình

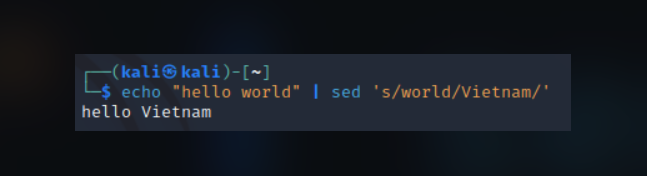
Mô tả được tạo tự động

### Tìm kiếm và thao tác văn bản

* Bài thực hành 15: grep



* Bài thực hành 16: sed



* Bài thực hành 17: cut

Ảnh có chứa văn bản, trong nhà, ảnh chụp màn hình, màu bạc

Mô tả được tạo tự động

* Bài thực hành 18: awk

Ảnh có chứa văn bản, màn hình, ảnh chụp màn hình, thiết bị điện tử

Mô tả được tạo tự động

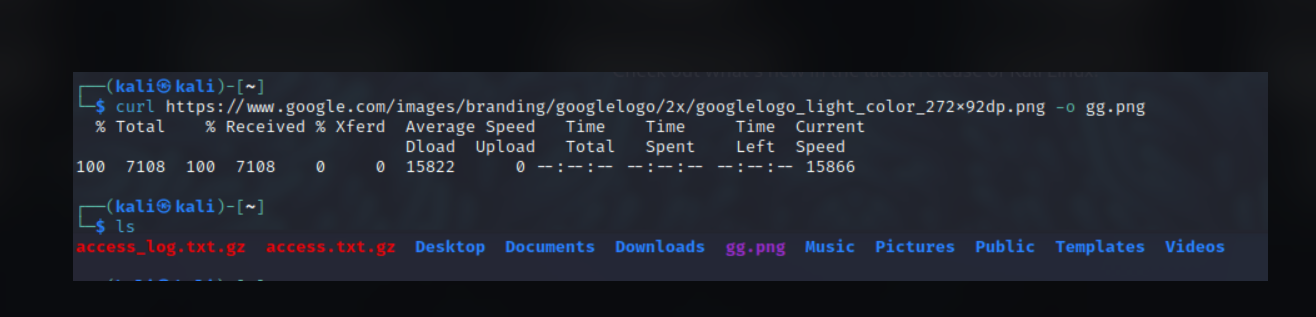
### Tải tập tin

* Bài thực hành 19: wget

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Bài thực hành 20: curl



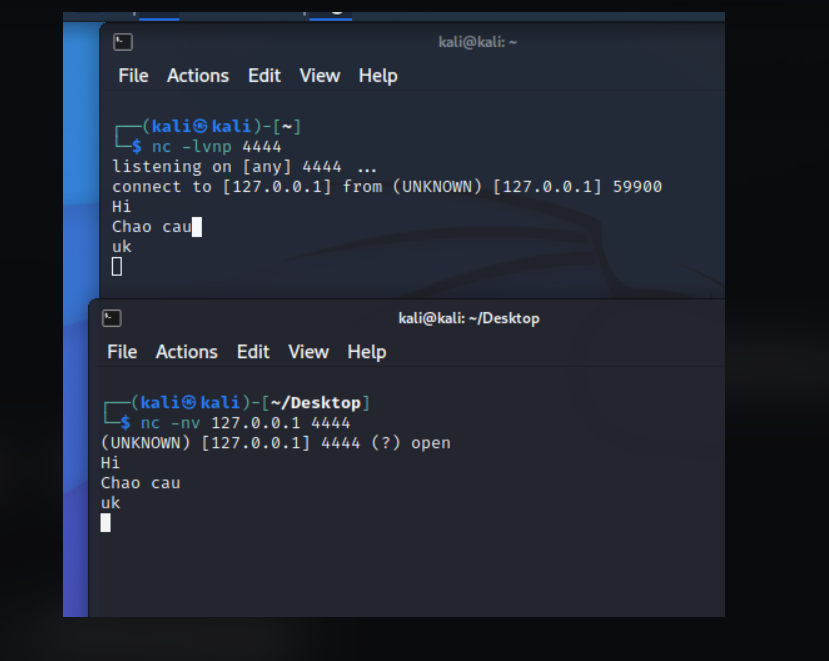
## Các công cụ cần thiết

### Netcat

* Bài thực hành 21: Kết nối TCP/UDP Port



* Bài thực hành 22: Lắng nghe trên TCP/UDP Port



* Bài thực hành 23: Trao đổi tập tin với Netcat

Ảnh có chứa văn bản

Mô tả được tạo tự động

Ảnh có chứa văn bản

Mô tả được tạo tự động

Ảnh có chứa văn bản

Mô tả được tạo tự động

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Bài thực hành 24: Quản trị từ xa với Netcat
* Ảnh có chứa văn bản

  Mô tả được tạo tự động

Ảnh có chứa văn bản

Mô tả được tạo tự động

### PowerShell

# Bài tập về nhà

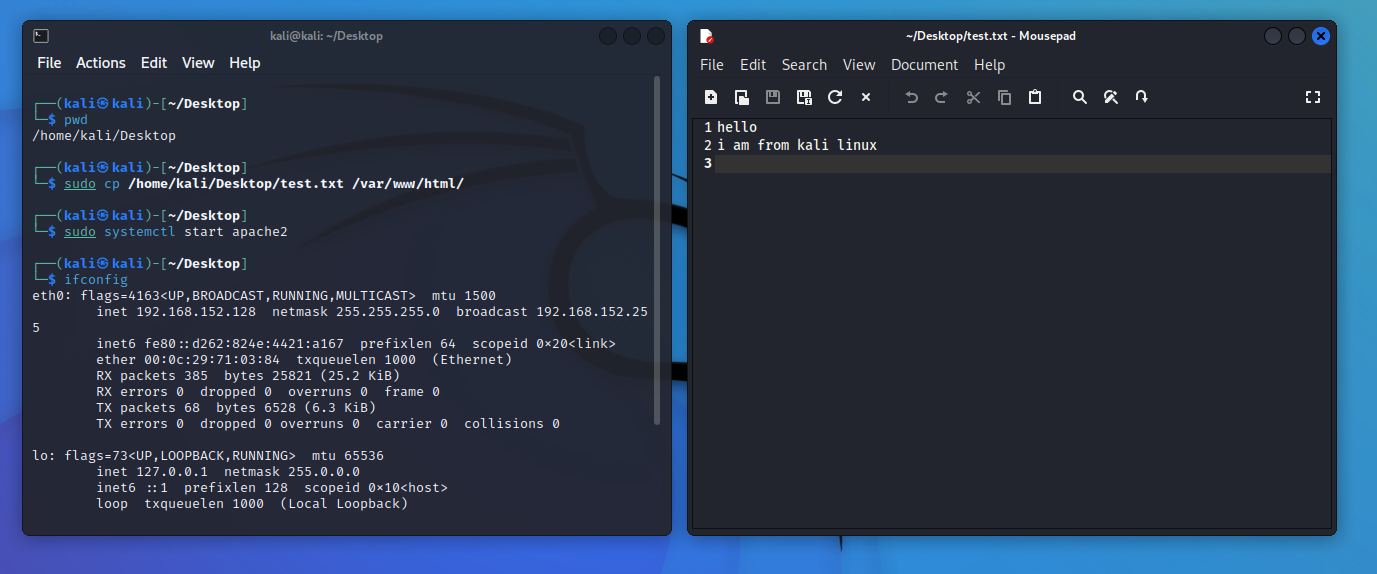
* Câu 1: Sử dụng lệnh which để xác định ví trị lưu trữ của lệnh pwd.

### Ảnh có chứa văn bản Mô tả được tạo tự động

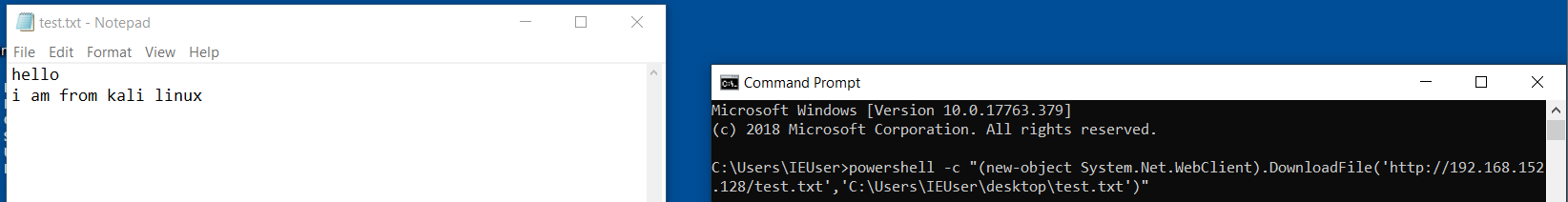
- Câu 2: Sử dụng lệnh locate để xác định ví trí lưu trữ wce32.exe

### Ảnh có chứa văn bản Mô tả được tạo tự động

* Câu 23.1: Thực hiện trao đổi tập tin sử dụng powershell



* Mang file test.txt vào vị trí thư mục gốc của apache web server
* Việc truyền file giữa 2 máy là download file từ máy kali với giao thức http
* Bên phải là nội dung file test.txt

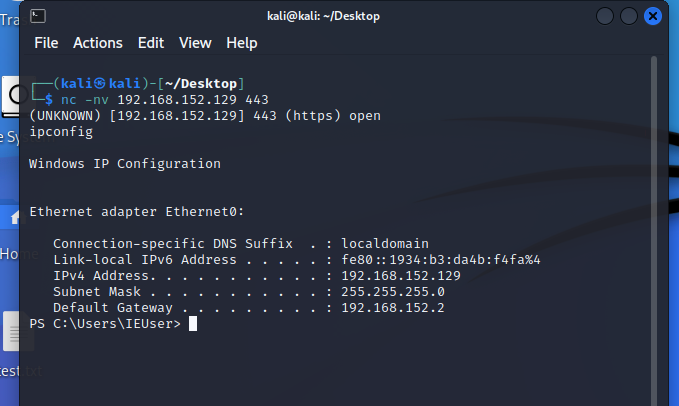


* Sau khi sử dụng câu lệnh trên ở cmd sử dụng powershell để truyền file giữa 2 máy thì sẽ có được file test.txt bên máy Kali
* Câu 23.2: Bind shell sử dụng powershell

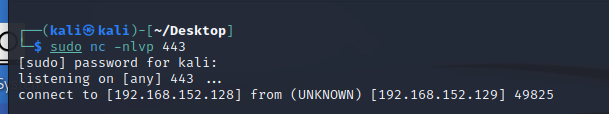
Ảnh có chứa văn bản

Mô tả được tạo tự động

* Khởi tạo listener với powershell
* Với thông số này nó sẽ nghe bất kỳ ip từ bất kỳ port vào



* Bên máy kali ta kết nối với máy window
* Câu 23.3: ReverseShell



* Bên máy kali ta dùng nc để nghe từ port 443

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Sau đó bên wondow tao viết câu lệnh sau để kết nối tới máy kali với ip của máy kali và port 443

Ảnh có chứa văn bản

Mô tả được tạo tự động

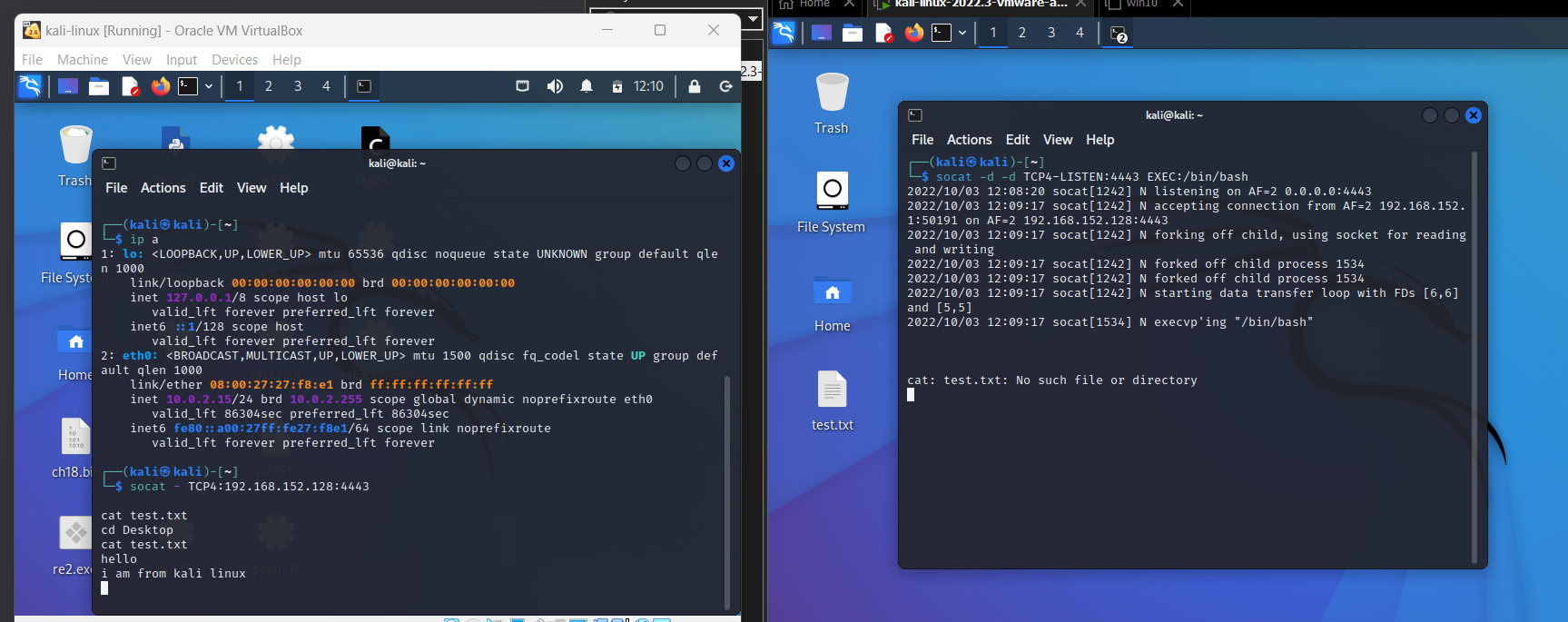
* Ta đã reverseshell thành công bên máy kali
* Câu 24: Ngoài netcat và powershell, còn cách nào có thể tạo ra được reverse shell và bind shell không? Cho một ví dụ.

+ Ta sử dụng socat

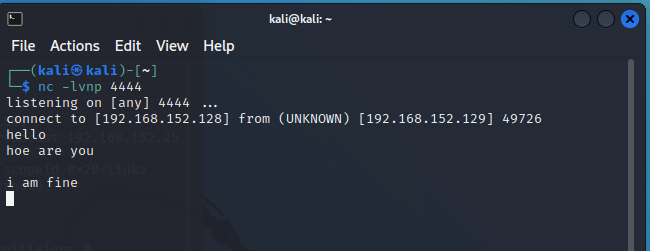
+ Ở ví dụ này ta sử dụng 2 máy kali với ip lần lượt là 10.0.2.15 và 192.168.152.128 là máy nạn nhân

+ Ở máy nạn nhân ta sử dụng câu lệnh: socat -d -d TCP4-LISTEN:4443 EXEC:/bin/bash

+ Ở máy attacker ta sử dụng câu lệnh : socat – TCP4:192.168.168.130:4443



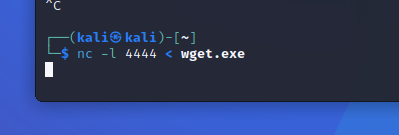
* Triển khai ứng dụng chat đơn giản trên 2 máy Kali và Windows 10. Và trả lời các câu hỏi sau:



Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ứng dụng chat đơn giản sử dụng netcat để kết nối giữa 2 máy win 10 và linux
* Câu 17: Máy chủ nào sẽ đóng vai trò là server?
* Máy sẽ đóng vai trò là server là máy linux sẽ lắng nghe bất cứ địa chỉ nào được kết nối tới port 4444
* Câu 18: Máy chủ nào sẽ đóng vai trò là client?
* Máy đóng vai trò là client là máy win 10 sẽ thực hiện kết nối tới máy linux thông qua địa chỉ ip của máy linux và port 4444
* Câu 19: .Nếu khai báo lệnh “nc -lvnp 4444” thì thật chất, port 4444 được mở ở máy nào?
* Port sẽ được mở ở máy thực hiện câu lệnh để có thể lắng nghe các kết nối tới port đó
* Câu 20: Thực hiện chuyển tập tin wget.exe trên máy Kali sang máy Windows 10.



* Trên máy kali

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Trên máy win 10 ta thấy xuất hiên file wget.exe được gửi từ máy kali
* Câu 21: Thực hiện lại chi tiết kịch bản Reverse Shell và Bind Shell sử dụng netcat

+ Bind shell

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Trên máy win 10 ta thực hiện lắng nghe trên port 4444 do kẻ tấn công là máy kali tạo ra

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Kẻ tấn công chỉ việc kết nối tới port đã tạo ra và sử dụng ip của máy nạn nhân là có thể tấn công thành công

+ Reverse shell

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Trên máy attacker ta thực hiện lắng nghe ở một cổng bất kỳ (4444)

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Trên máy nạn nhân ta thực hiện kết nối tới port đó và cung cấp cho kẻ tấn công trình cmd để có thể điều khiển từ xa
* Câu 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

|  |  |
| --- | --- |
| Reverse shell | Bind shell |
| * Ưu điểm   +Kẻ tấn công sẽ thực hiện nghe ở một cổng bất kỳ mà nạn nhân thường truy cập  +Kết nối với các máy chủ được bảo vệ bởi firewall hoặc hệ thống bảo mật mạng   * Nhược điểm   + Máy nạn nhận có thể chỉ cho phép 1 số ip hoặc chỉ hoạt động ở 1 số cổng cụ thể mà dịch vụ yêu cầu | * Ưu điểm   +Khó bị phát hiện khi máy mình thực hiện nghe ở một port mà attacker tạo ra  +Có thể để lại backdoor   * Nhược điểm   + Nạn nhận thường sẽ ở sau bộ định tuyến NAT làm cho việc bind shell thông qua mạng WAN khó thực hiện  + binding socket phải xem xét kĩ lưỡng |
| * Ta nên sử dụng khi máy nạn nhân có tường lửa * Không biết ip của máy nạn nhân | * Khi đã biết được ip của máy nạn nhân * Khi muốn đặt backdoor và không có thiết lập lệnh và kiểm soát |

* Câu 14: Hãy cho biết đường đẫn thực thi của 2 lệnh wget và curl?

+ Lệnh wget: <https://github.com/blakduk/ahihi/raw/master/access_log.txt.gz>

+ Lệnh curl:

<https://www.google.com/images/branding/googlelogo/2x/googlelogo_light_color_272x92dp.png>

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

+ Lệnh wget là một lệnh truyền đơn giản còn curl sẽ cung cấp nhiều tiện ích hơn

+ curl cung cấp thư viện libcurl có thể được mở rộng thành các ứng dụng GUI, còn wget là một tiện ích dòng lệnh đơn giản

+ wget hỗ trợ ít giao thức hơn curl

+ wget có sẵn trong linux còn curl có sẵn trong window

+ curl hỗ trợ HTTP 2 chiều trong khi wget chỉ hỗ trợ POST

+ wget không hỗ trợ SOCKS

+ wget cần cài đặt gnulib

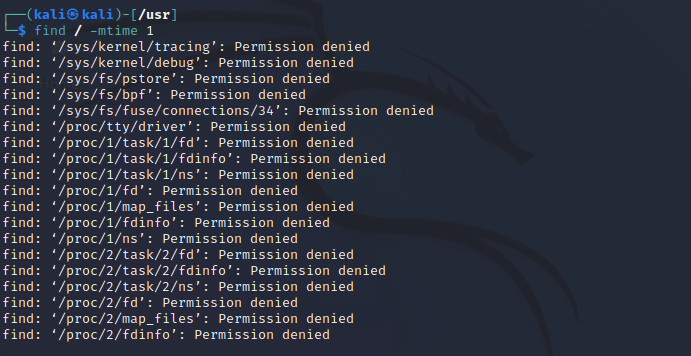
+ trong curl các tính năng như cookie, timestamp, và chuyển hướng được bật mặc dịnh còn wget phải được chỉ định bật từng cái

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

+ Có thể dùng lệnh curl để thay đổi các HTTP header

+ Vd: $ curl -H "Agent: linuxtect" <https://www.linuxtect.com>

* Câu 3: 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



* Câu 4: Liệt kê các port đang được mở trên kali linux

A screenshot of a computer

Description automatically generated with medium confidence

* Câu 6: Ngăn dịch vụ SSH chạy cùng với hệ thống lúc khởi động

Text

Description automatically generated

* Câu 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 được lưu trữ ở file lịch sử dưới dạng .bash\_history

Ưu điểm:

+ giúp tăng hiệu suất công việc

+ được sử dụng để điều tra, xử lý các sự cố bảo mật.

Nhược điểm:

Do phải lưu trữ nên tốn tài nguyên, bộ nhớ.

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

+ Có thể chỉ dịnh một hoặc nhiều lệnh không bao giờ được ghi vào tệp lịch sử với biến $HISTIGNORE.

Ví dụ: **export HISTIGNORE="cd”**

Với ví dụ trên lệnh history sẽ không lưu lại lịch sử với câu lệnh cd.

* Câu 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 cách sử dụng tiện ích history expansion, chúng ta còn có thể dùng phím mũi tên ↑↓ để quay trở lại các lệnh ta đã nhập. Ngoài ra chúng ta còn có thể sử dụng phím Tab để hiển thị một số gợi ý.