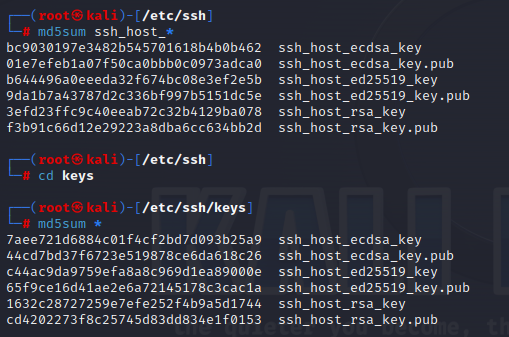
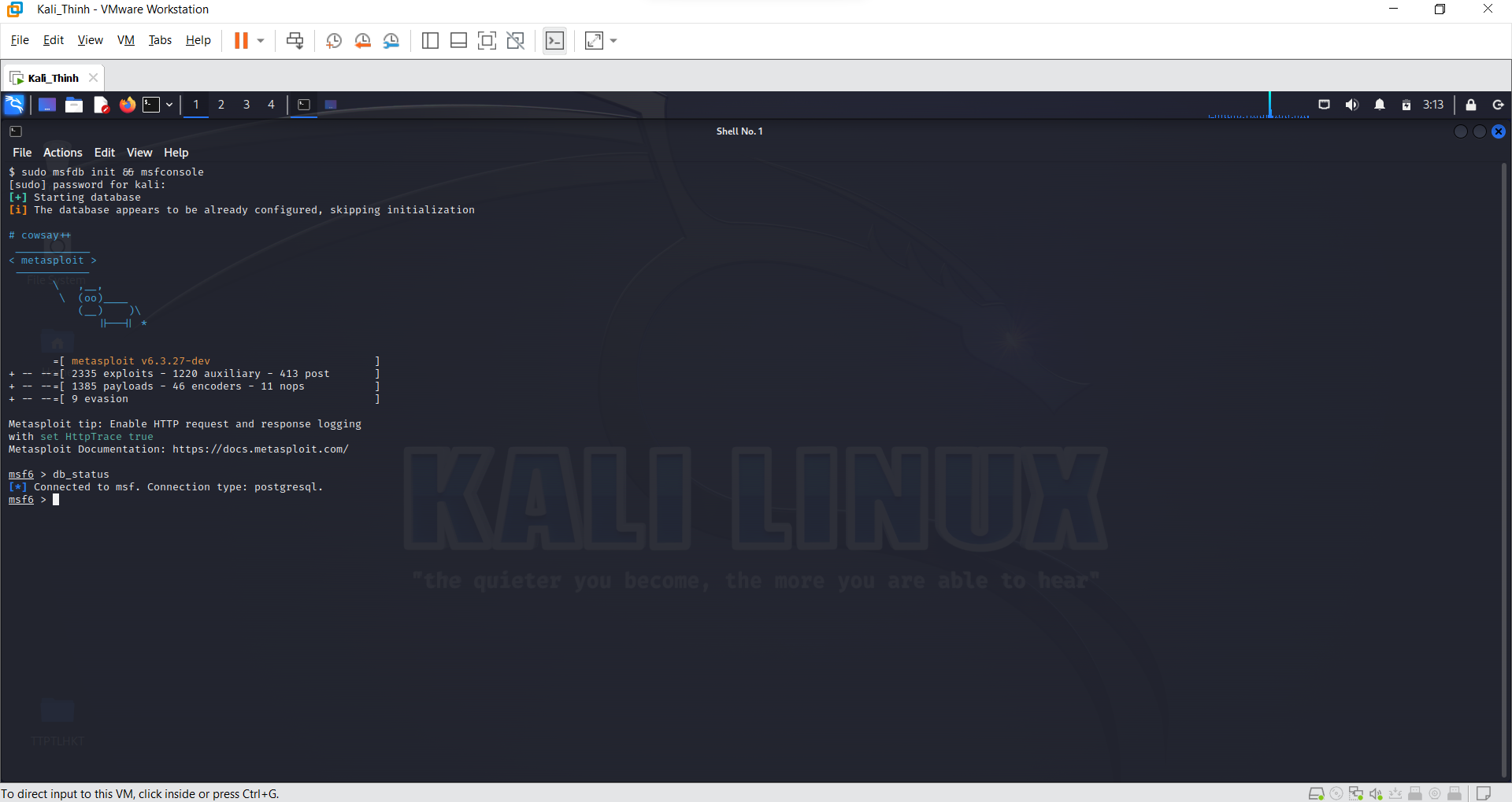
2033210464 – Nguyễn Trần Như Thịnh

**LAB 1**

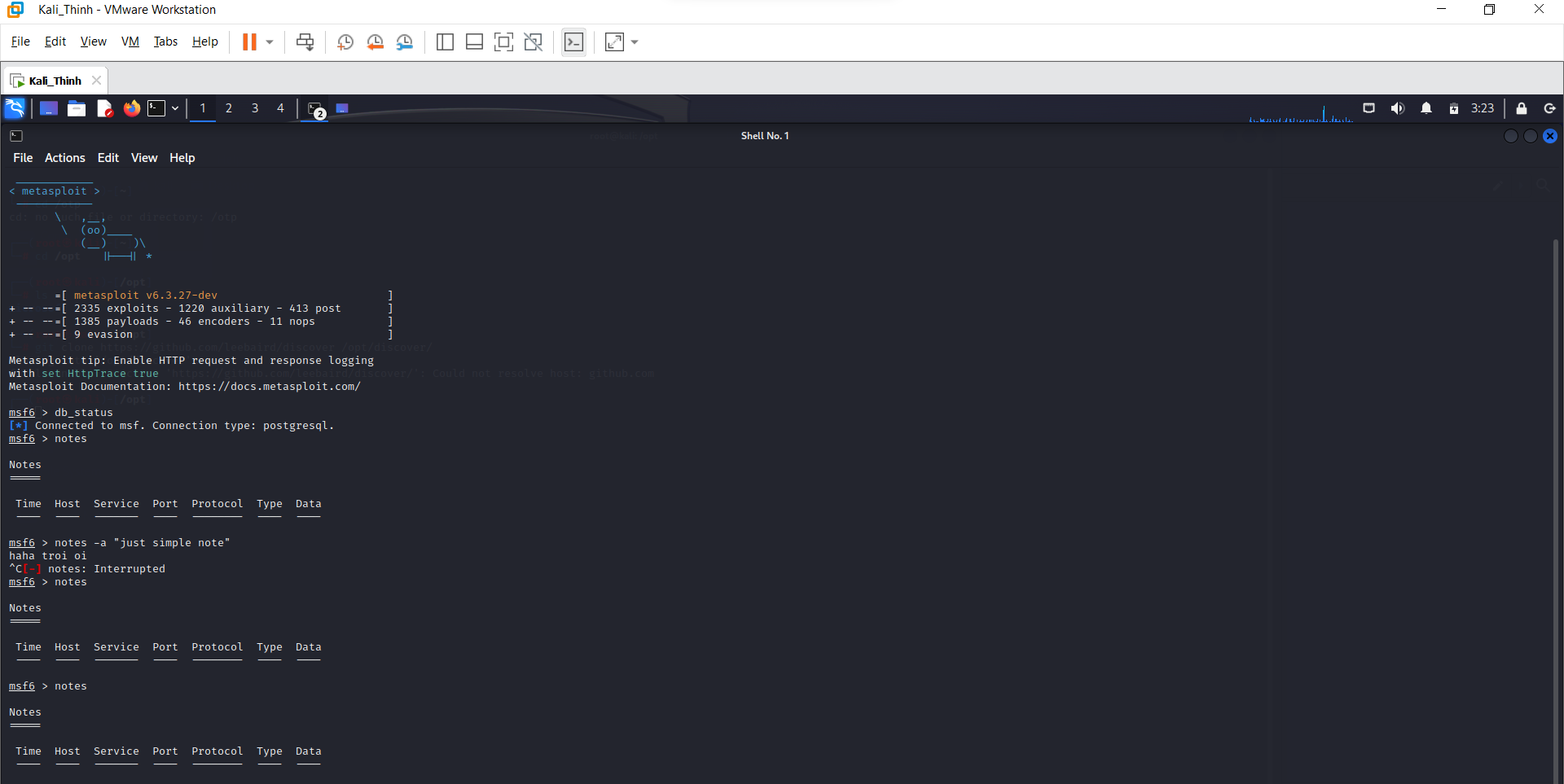
### **perform an md5 sum**



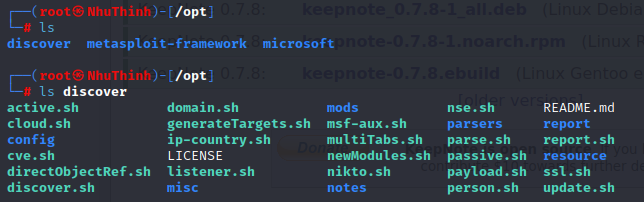
### **ISSUE THE DB\_STATUS COMMAND**



### **OPEN YOUR METASPLOIT NOTES**

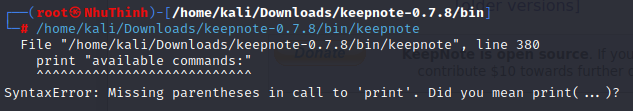


### **CLONE THE DISCOVER DIRECTORY**



### **Recreate the following node layout**

Em không tải được KeepNote vì nó không còn khả dụng trên Kali 2019 trở đi



Step 1: File > New Notebook.

Step 2: Type a name “mham\_notes” and choose location to save

Step 3: Choose “mham\_notes” folder and create new folders: Info Gathering, Scanning, Exploitation, Maintaining Access, Covering Tracks

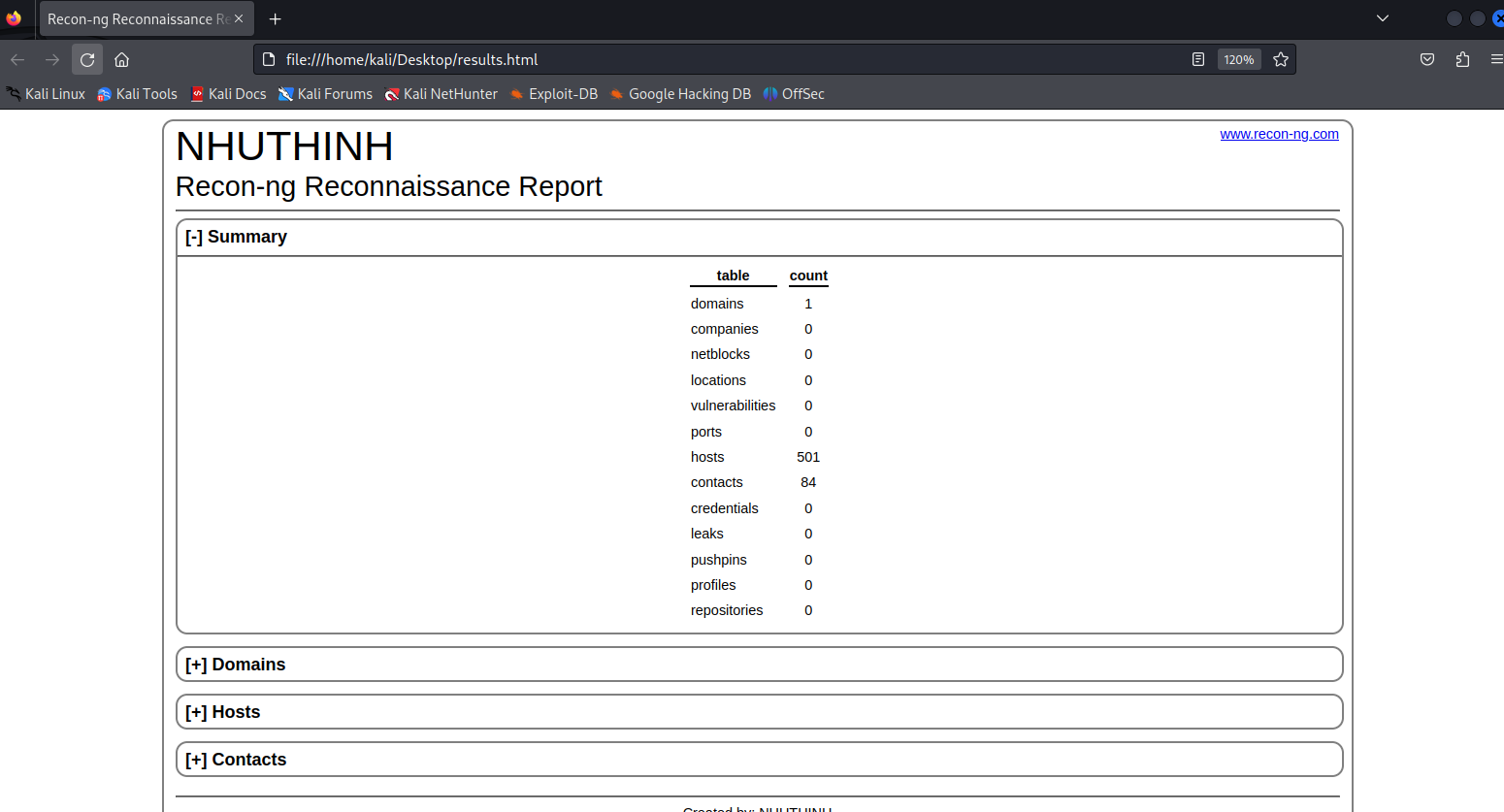
Step 3: Choose “mham\_notes” folder and create new folders: Info Gathering, Scanning, Exploitation, Maintaining Access, Covering Tracks

Step 4: Choose “: Info Gathering” folder and create new folders: Footprinting, Recon.

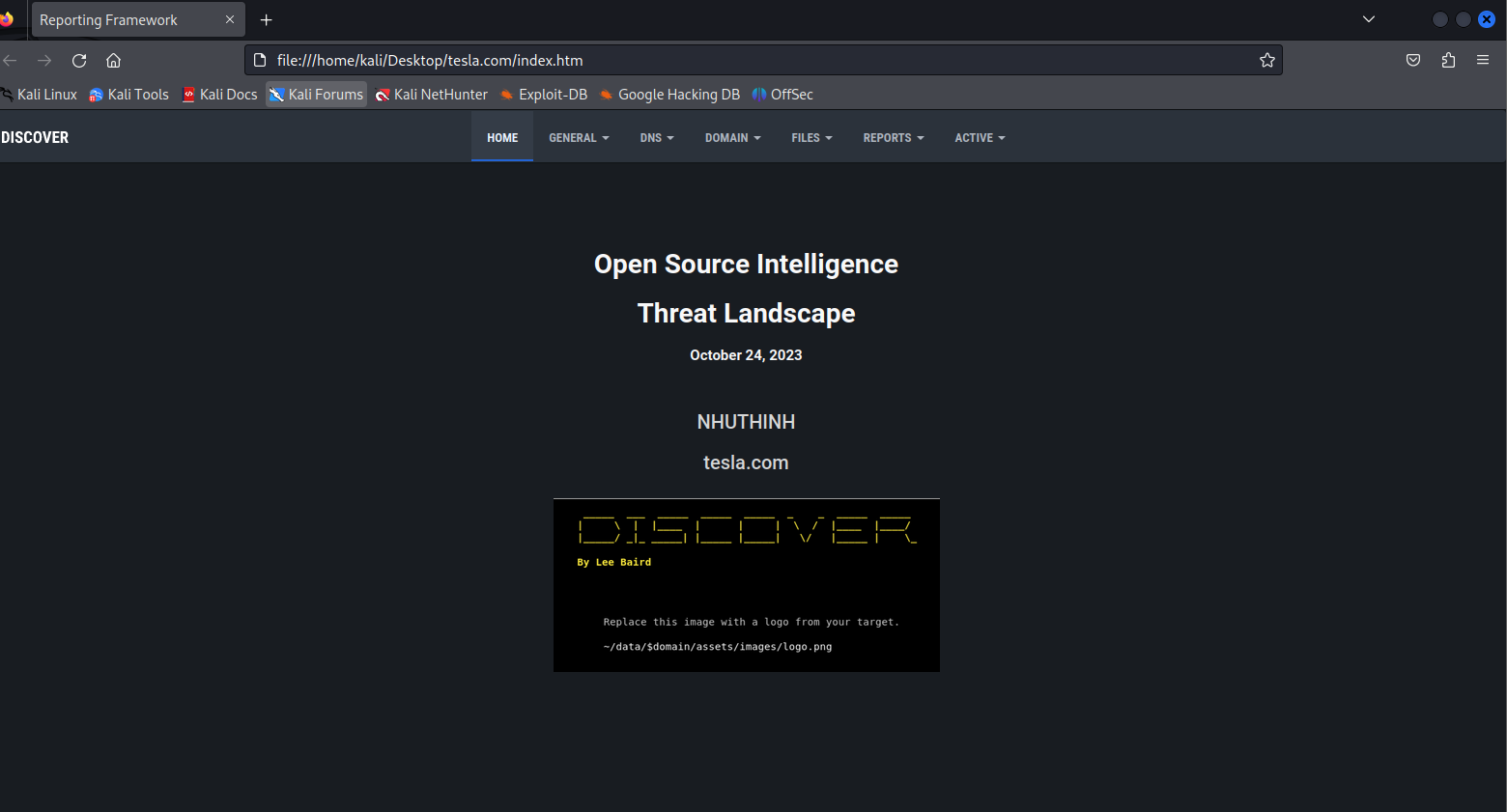
Step 5: Change note icon

**LAB 2**

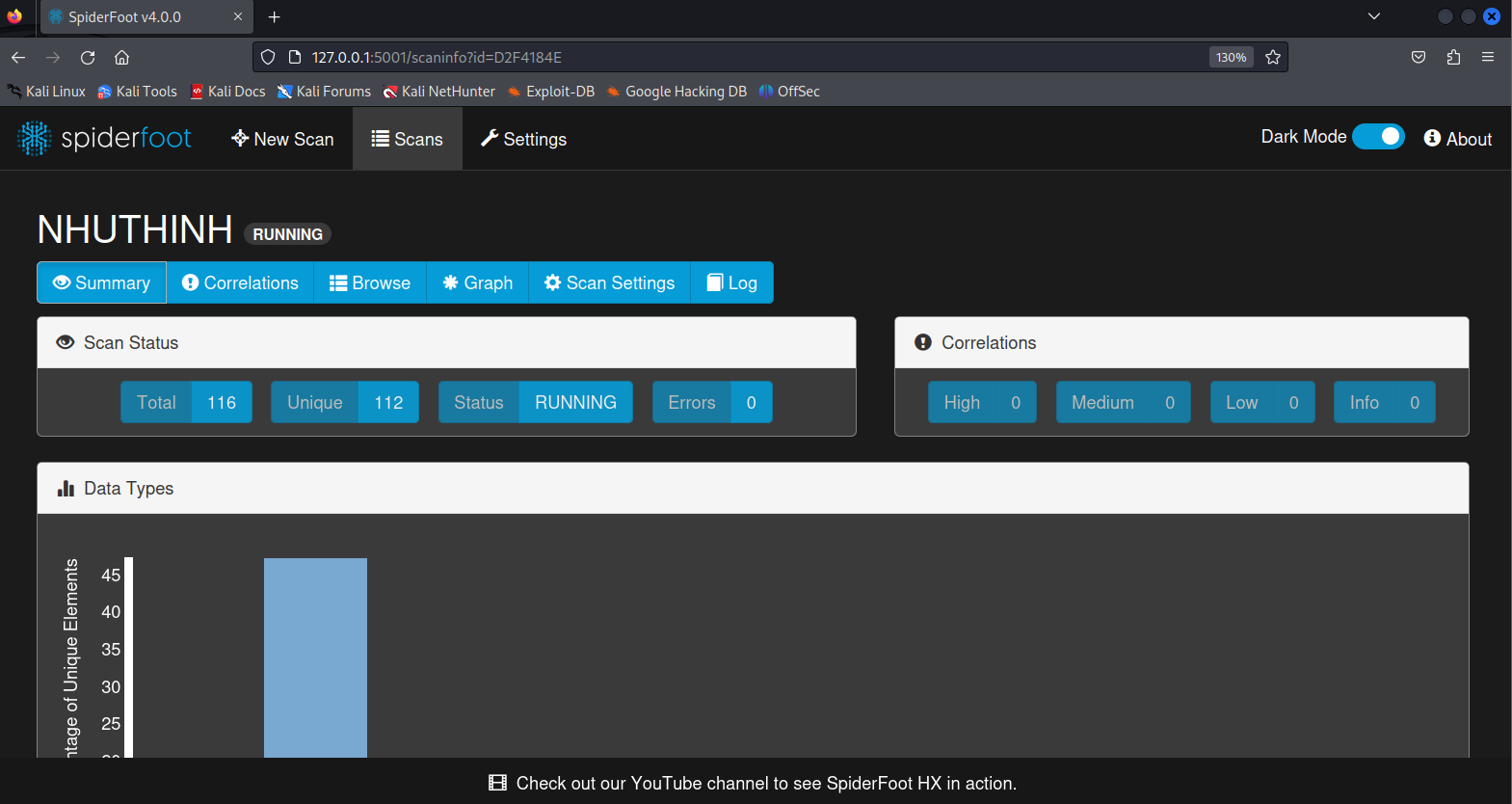
### **Recon-NG**



### **Discover Scripts**

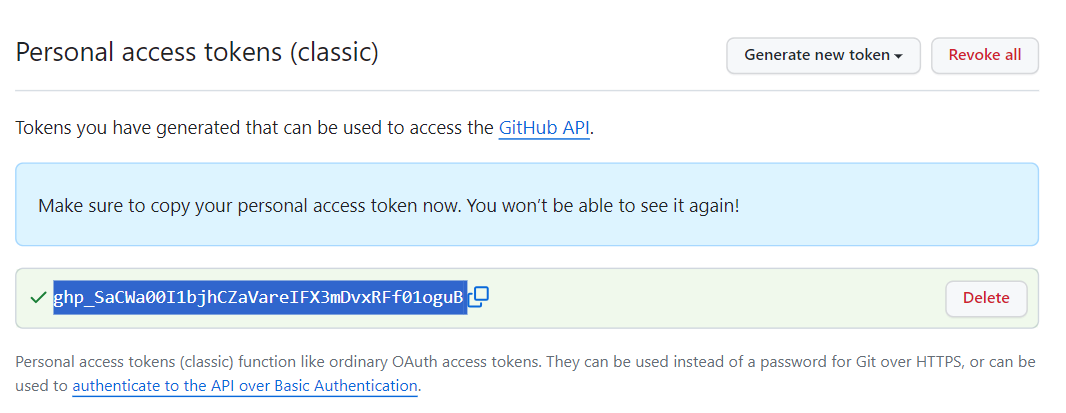


### **SpiderFoot**

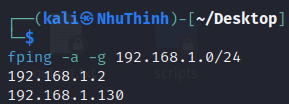


**LAB 3**

### **GitRob**



### **fPING**



FOOTPRINTING AND RECONNAISANCE

# LAB 1. PERFORM FOOTPRINTING THROUGH SEARCH ENGINES

## 1.1. GATHER INFORMATION USING ADVANCED GOOGLE HACKING TECHNIQUES

**1.** Loại trừ một từ khỏi kết tìm kiếm: “[keyword]” –”[keyword loại trừ]”

*Trước khi thêm lệnh:*

A screenshot of a computer

Description automatically generatedSau *khi thêm lệnh: Kết quả trả về đầu tiên chứa tử “cổng” đã biến mất*

A screenshot of a computer

Description automatically generated

**2.** Tìm kết quả từ một trang web cụ thể: site:[website]

*Trước khi thêm lệnh: Các kết quả trả về từ website Youtube*

A screenshot of a video

Description automatically generated

*Sau khi thêm lệnh: Các kết quả từ website nhaccuatui xuất hiện*

A screenshot of a web page

Description automatically generated

**3.** Tìm các page của website có chưa từ khóa: site:[website] [keyword]

A screenshot of a computer

Description automatically generated

*Kết quả trả về đúng website và có keyword tương ứng*

**4.** Hiển thị các trang web có URL chứa toàn bộ từ khóa hoặc cụm từ: allinurl:keyword

Tìm kiếm: allinurl:hỗn loạn -> và thu được các kết quả tương ứng

A black and blue rectangle with white text

Description automatically generated



**5.** Tìm kiếm các loại tệp cụ thể: filetype:[extension]

*Trước khi dùng lệnh:*

A screenshot of a computer

Description automatically generated

Sau khi dùng lệnh: các kết quả trả về là các tập tin power point

A screenshot of a computer

Description automatically generated

**6.** Tìm từ cụm khóa trong tiêu đề trang web: allintitle:[keyword group]

A screenshot of a computer

Description automatically generated

*Các kết quả trả về đều có tiêu đề là “nàng thơ”*

**7.** Tìm cụm từ hoặc từ khóa trên trang web: allintext:[phases or keyword]

A screenshot of a web page

Description automatically generated

*Kiểm tra nội dung các kết quả thì đều có các từ khóa*

## 1.2. GATHER INFORMATION FROM VIDEO SEARCH ENGINES

Sử dụng youtube vì nó phổ biến, vào một video bất kỳ và sao chép đường dẫn

A screenshot of a computer

Description automatically generated

Vào công cụ trực tuyến sau



Nhập đường dẫn và trang sẽ hiển thị các thông tin thống kê từ video

A screenshot of a video game

Description automatically generated

Bao gồm cả thống kê doanh thu

A screenshot of a video game

Description automatically generated

## 1.3 GATHER INFORMATION FROM FTP SEARCH

Sử dụng công cụ tìm kiếm lập chỉ mục NAPALM FTP để trích xuất thông tin FTP quan trọng về mục tiêu



Thu thập được các kết quả FTP và có thể download về

A screenshot of a computer

Description automatically generated

## 1.4 GATHER INFORMATION FRO M IOT SEARCH ENGINES

Thu thập thông tin về các thiết bị IOT dễ bị tấn công trong tổ chức mục tiêu sử dụng công cụ tìm kiếm Shodan IoT



Thu thập được thông tin thành công của tổ chức Micrsoft

A screenshot of a computer

Description automatically generated

# 2. PERFORM FOOTPRINTING THROUGH WEB SERVICES

## 2.1. FIND THE COMPANY'S DOMAINS AND SUB-DOMAINS USING NETCRAFT

Vào tool siteport của NETCRAFT theo đường dẫn

A screenshot of a computer

Description automatically generated

Trang web đó đang chạy cái gì? trang xuất hiện. Để trích xuất thông tin liên quan đến trang web của tổ chức như cơ sở hạ tầng, công nghệ được sử dụng, tên miền phụ, nền tảng, mạng, v.v

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Còn có thể xem thông tin về các sub-domains

A screenshot of a computer

Description automatically generated

## 2.2. GATHER PERSONAL INFORMATION USING PEEKYOU ONLINE PEOPLE SEARCH SERVICE

Tại đây, chúng ta sẽ thu thập thông tin về một người từ tổ chức mục tiêu bằng cách thực hiện tìm kiếm người bằng dịch vụ tìm kiếm người trực tuyến PeekYou.



Nhập tên và tiểu bang, sau đó thu được các thông tin tương ứng

A screenshot of a computer

Description automatically generated

## 2.3. GATHER AN EMAIL LIST USING THEHARVESTER

Vào kali và gõ lệnh sau và trong lệnh này, -d chỉ định tên miền hoặc tên công ty cần tìm kiếm, -I chỉ định số lượng kết quả cần truy xuất và -b chỉ định nguồn dữ liệu.



Thu được 18 kết quả về Email, nó cũng sẽ trích xuất các máy chủ của công ty mục tiêu

A screenshot of a computer screen

Description automatically generated

## 2.4. DETERMINE TARGET OS THROUGH PASSIVE FOOTPRINTING



Nhập vào một trang web hay một địa chỉ mục tiêu, và nhận được kết quả hệ điều hành trả về

A screenshot of a computer

Description automatically generated

# 3. GATHER PERSONAL INFORMATION FROM VARIOUS SOCIAL NETWORKING SITES USING SHERLOCK

Cài đặt từ github

A computer screen shot of a program

Description automatically generated

Chạy lệnh sau và nhập họ và tên để tra cứu từ các trang web

A computer screen with white text and numbers

Description automatically generated

A computer screen shot of a program

Description automatically generated

Thu về được gần 300 kết quả



# 4. PERFORM WEBSITE FOOTPRINTING

## 4.1. GATHER INFORMATION ABOUT A TARGET WEBSITE USING PING COMMAND LINE UTILITY

Ping default sẽ trả về địa chỉ IP

A screen shot of a computer

Description automatically generated

Phản hồi trả về gói cần được phân mảnh nhưng được đặt DF -> khung quá lớn để có trên mạng và cần được phân mảnh. Gói không được gửi vì đã sử dụng khóa chuyển -f với lệnh ping và lệnh ping đã trả về lỗi

A computer screen with white text

Description automatically generated

Sau vài lần thử đã tìm ra được max và min