# Cài đặt và làm quen với các công cụ trên Kali Linux

## Cài đặt Kali Linux, thêm user với mã sinh viên và gán quyền sudo

* Giao diện Kali Linux sau khi cài đặt:



Hình : Giao diện Kali Linux

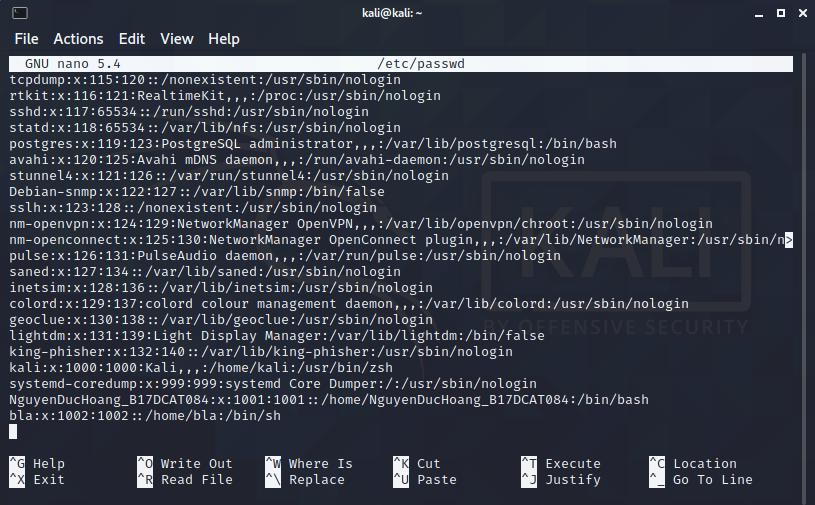
* Command tạo mới user:

Sudo useradd NguyenDucHoang\_B17DCAT084

* Command tạo mật khẩu cho user:

Sudo passwd NguyenDucHoang\_B17DCAT084

* Đổi Shell cho user mới thông qua file /etc/passwd:
  + Sudo nano /etc/passwd
  + Tìm đến dòng chứa thông tin về user mới tạo
  + Chỉnh sửa /bin/sh thành /bin/bash
  + Lưu lại thông qua Ctrl+X

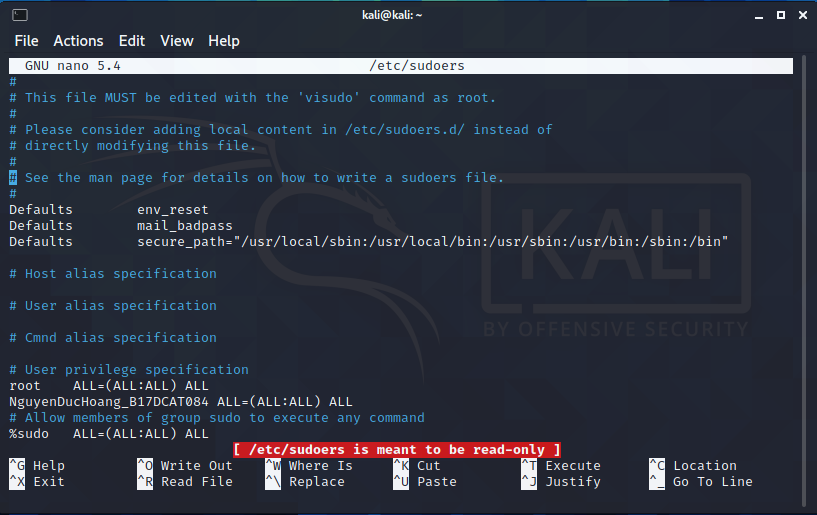


Hình : Đổi Shell cho user mới tạo

* Gán quyền sudo cho user mới:
  + Sudo nano /etc/sudoers
  + Thêm dòng mới vào file

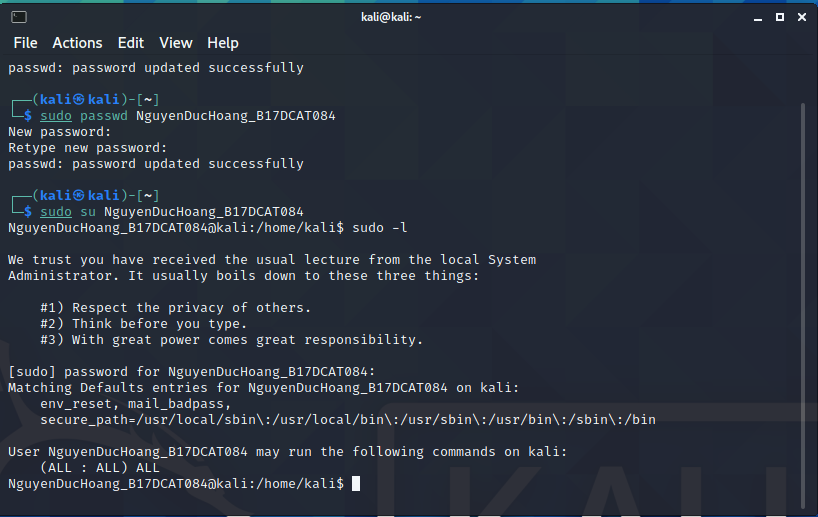
NguyenDucHoang\_B17DCAT084 ALL=(ALL:ALL) ALL

* + Lưu lại thông qua Ctrl+X



Hình : Thêm quyền sudo cho user thông qua /etc/sudoers

* Login bằng user mới tạo để kiểm tra:



Hình : Tạo mới user với quyền sudo thành công

## Tìm hiẻu các công cụ có trong Kali Linux

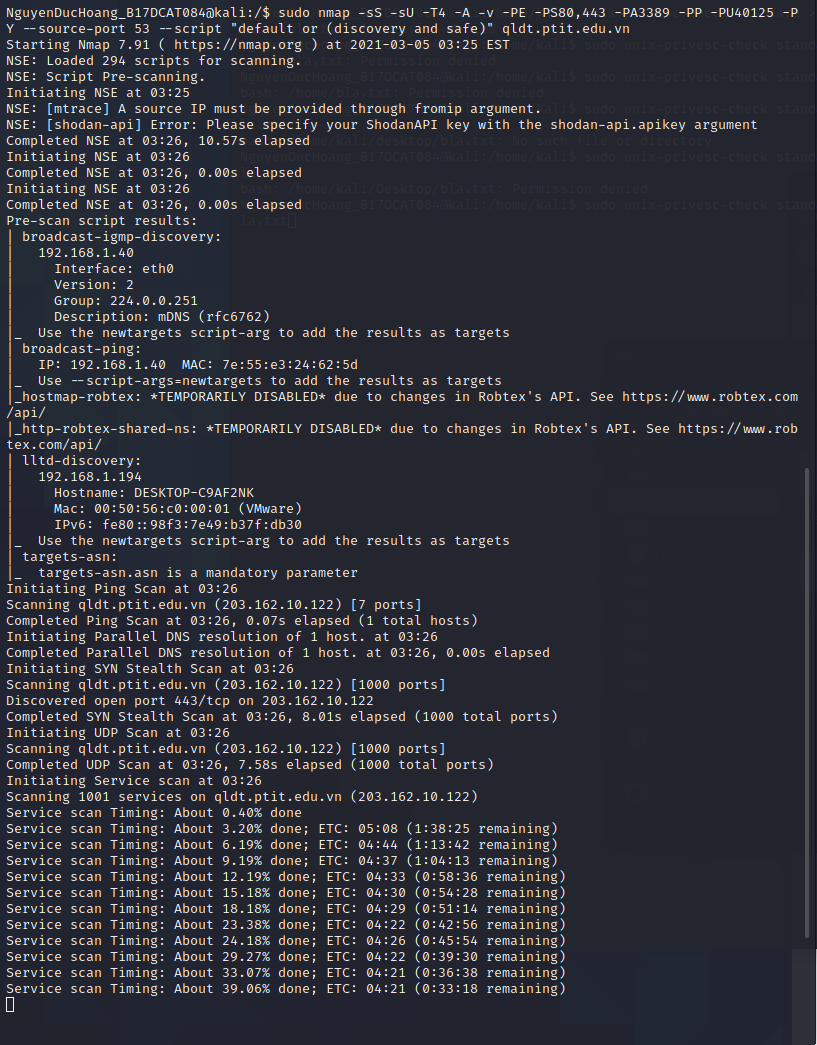
### Information Gathering: Nmap

* Nmap (tên đầy đủ Network Mapper) là một công cụ bảo mật mã nguồn mở được phát triển bởi Floydor Vaskovitch. Nmap được sử dụng để xác định xem thiết bị nào đang chạy trên hệ thống, cũng như tìm kiếm ra các máy chủ có sẵn và các dịch vụ mà các máy chủ này cung cấp, đồng thời dò tìm các cổng mở và phát hiện các nguy cơ về bảo mật.
* Command:

nmap -sS -sU -T4 -A -v -PE -PS80,443 -PA3389 -PP -PU40125 -PY --source-port 53 --script "default or (discovery and safe)" <target\_ip>

Trong đó:

* + -sS: Quét các cổng TCP
  + -sU: Quét các cổng UDP
  + -T4: Cài timing template là 4
  + -v: Tăng độ chi tiết của kết quả
  + -PE: Thăm do bằng cách gửi các gói tin ICMP echo
  + -PP: Thăm do qua cách gửi các gói tin Timestamp
  + -PS80,443: Thăm dò các port thường sử dụng cho dịch vụ HTTP và HTTPS như 80, 443 bằng gói tin TCP SYN
  + -PA3389: Thăm dò port thường được sử dụng cho dịch vụ Remote Desktop trên Windows là 3389 bằng gói tin TCP ACK
  + -PU40125: Thăm dò port thường được sử dụng cho dịch vụ UDP ping như 40125 bằng UDP
  + -PY: Thăm dò bằng cách gửi các gói tin SCTP
  + --source-port 53: Gửi các gói tin bằng cổng 53 để tránh sự phát hiện của 1 số loại firewall
  + --script: Sử dụng NSE script để thực hiện các công việc tự động



Hình : Sử dụng công cụ Nmap

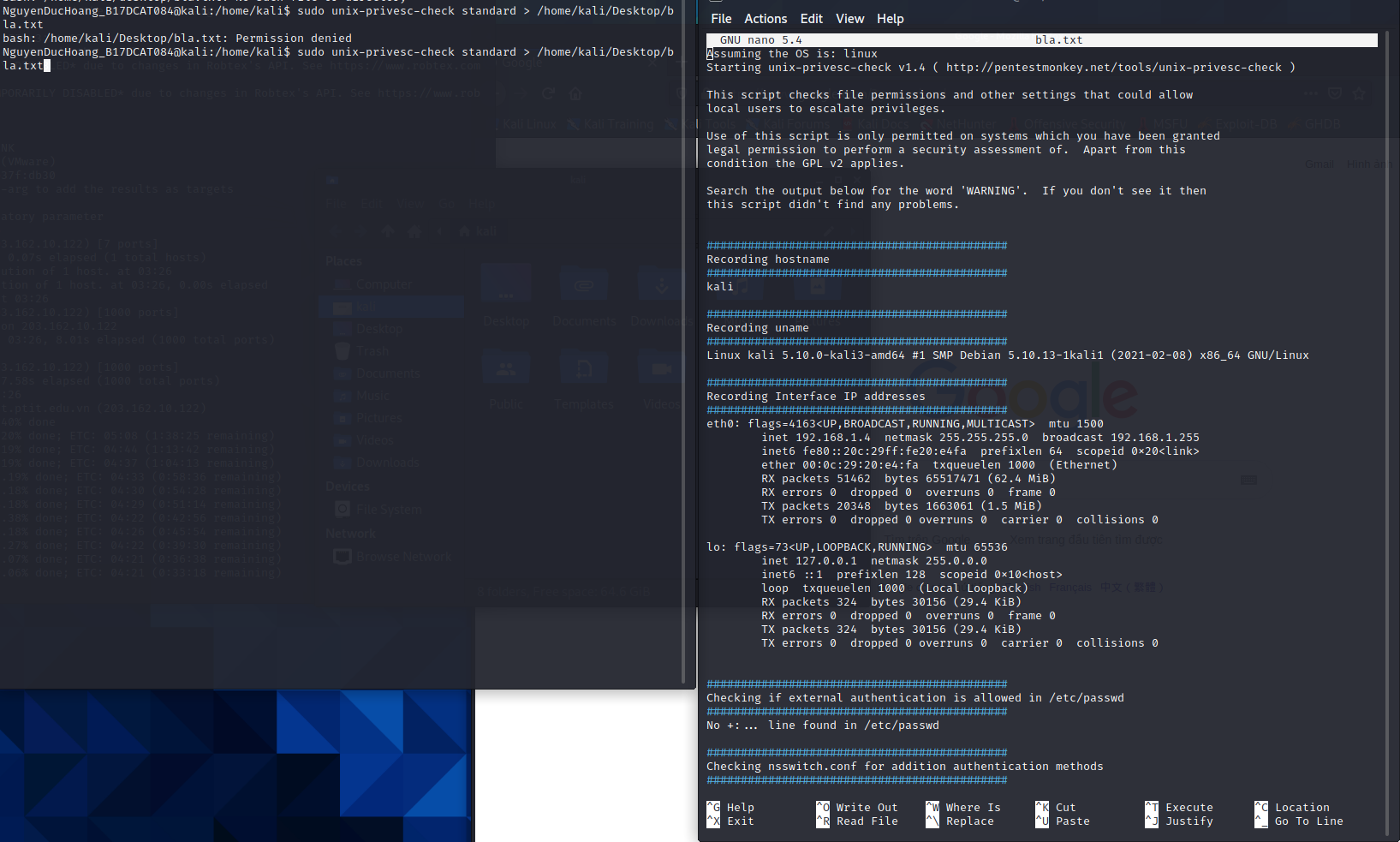
### Vulnerability Analysis: unix-privesc-check

* Công cụ rà quét các lỗ hổng cấu hình tồn tại trên hệ thống có thể dẫn tới việc leo quyền của người dùng (Privilege Escalation)
* Command:

unix-privesc-check <mode>

Trong đó mode có thể là một trong 2 giá trị:

* + Standard: Quét nhanh các cài đặt bảo mật.
  + Detail: Tương tự tuy nhiên công cụ sẽ kiểm tra thêm các quyền đọc ghi file.

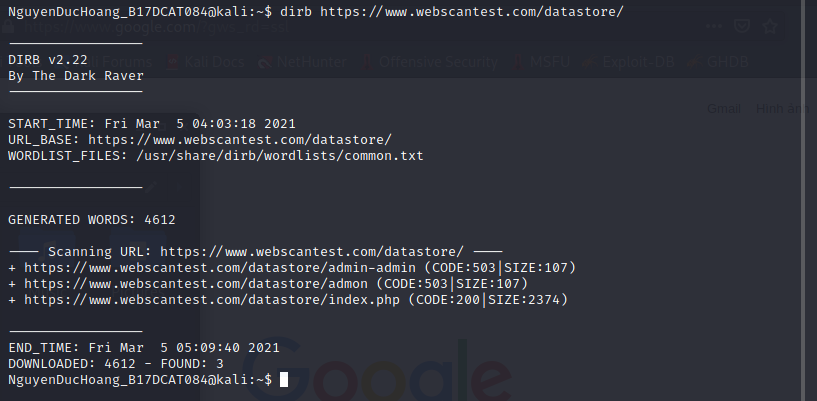


Hình : Sử dụng công cụ unix-privesc-check

### Web Application Analysis: dirb

* Dirb là công cụ rà quét web nhằm tìm ra các Web object đang tồn tại thông qua việc brute bằng từ điển.
* Command:

Dirb <Target>



Hình : Sử dụng công cụ Dirb

### Database Assessment: sqlmap

* Sqlmap là công cụ giúp rà quét lỗi SQL injection cũng như sinh payload khai thác trong trường hợp phát hiện lỗi.
* Command:
  + Xác định lỗi trong một trang Web:

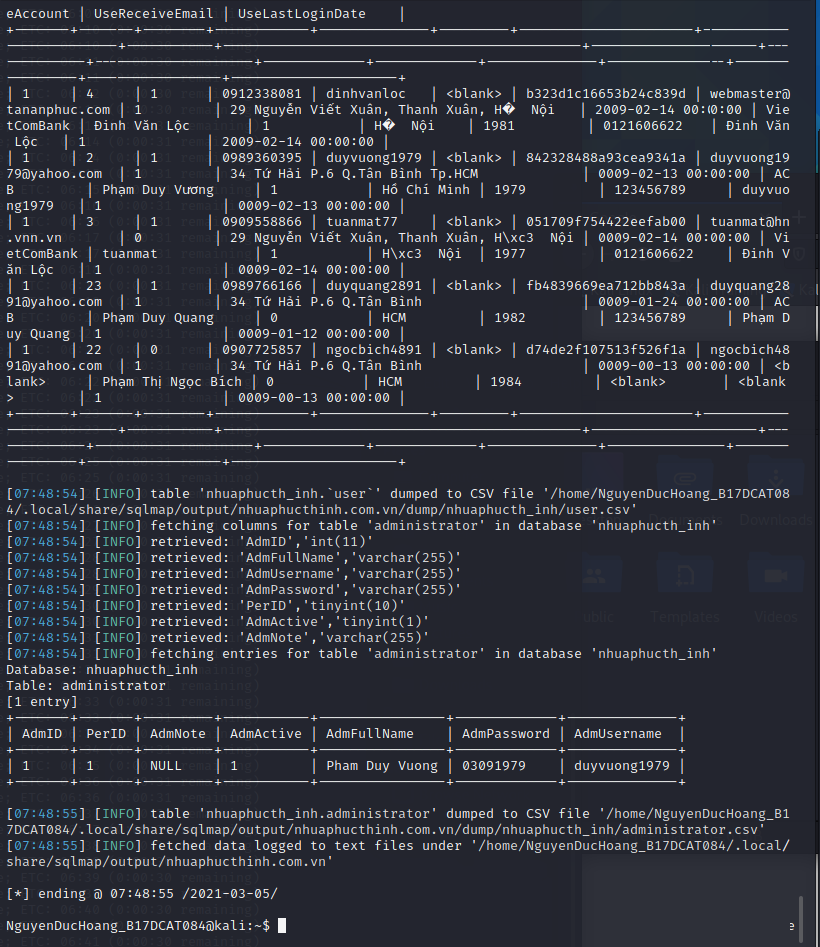
Sqlmap -u <Target>

* + Xác định các bảng có trong CSDL

Sqlmap -u <Target> --dbs

* + Dump toàn bộ dữ liệu

Sqlmap -u <Target> --dump <Tên bảng>



Hình : Sử dụng sqlmap khai thác lỗ hổng SQL injection trong ứng dụng web thực tế

### Password Attack: john

* John là công cụ sử dụng để bẻ khoá mật khẩu thông qua phương pháp từ điển hoặc bruteforce.
* Ví dụ command bẻ khoá mật khẩu file zip:
  + Lấy giá trị hash của mật khẩu file zip

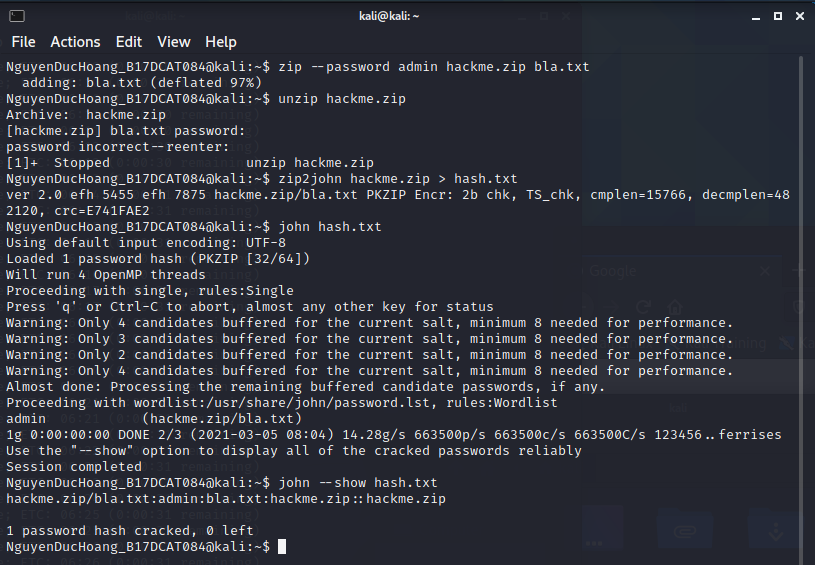
Zip2john <zip\_file> > hash.txt

* + Tìm kiếm giá trị băm mật khẩu trong từ điển có sẵn

John hash.txt

* + Hiển thị password trong trường hợp thành công

John –-show hash.txt



Hình : Sử dụng công cụ john bẻ khoá mật khẩu file zip

### Wireless Attack: aircrack-ng

* Aircrack-ng là một trong những công cụ cho phép bẻ khoá mật khẩu Wifi thông qua phương pháp bruteforce hoặc từ điển có sẵn.
* Command:

Aircrack-ng <file WAP handshake đã bắt> -w <thư viện password>

### Reverse Engineering: radare2

* Radare2 là một công cụ khá mạnh giúp hỗ trợ dịch ngược và phân tích mã trên nền UNIX.
* Command:
  + Khởi chạy công cụ:

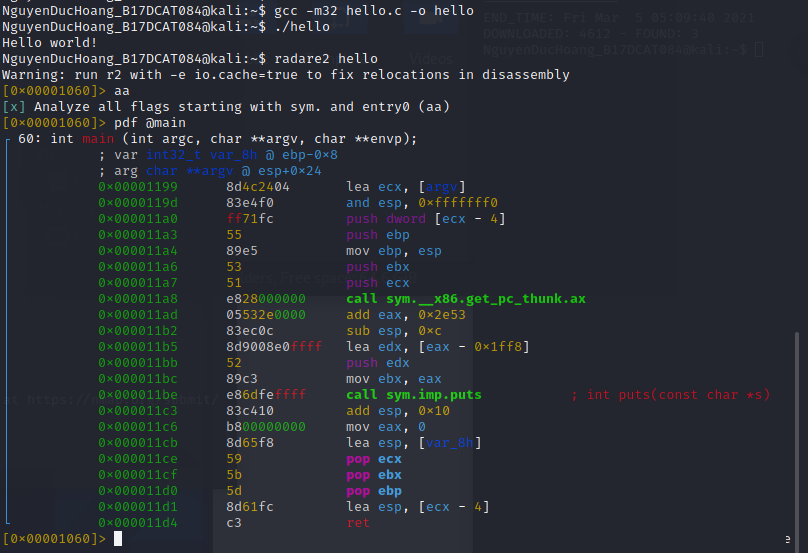
Radare2 <tên file>

* + Phân tích mã assembly của toàn bộ file vừa được chọn

Aa

* + Xem mã assembly của function nhất định

Pdf @<function name>

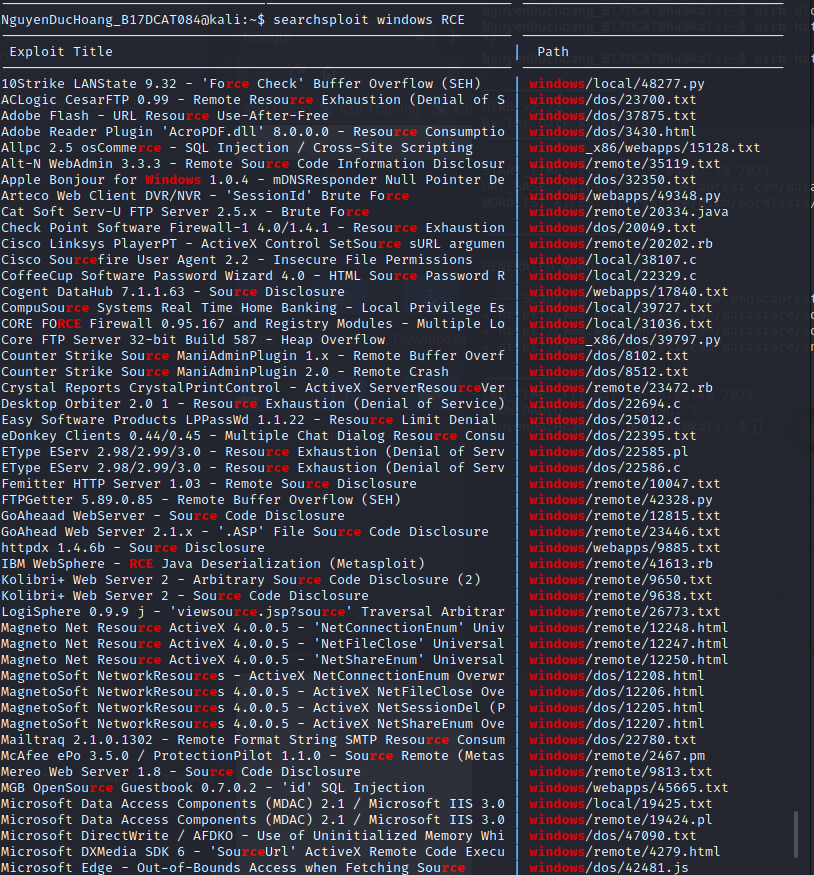


Hình : Sử dụng công cụ radare2 phân tích mã nguồn chương trình helloworld

### Exploitation Tools: searchsploit

* Searchsploit là công cụ tìm kiếm các payload khai thác và các phương thức exploit có sẵn trong database.
* Command:

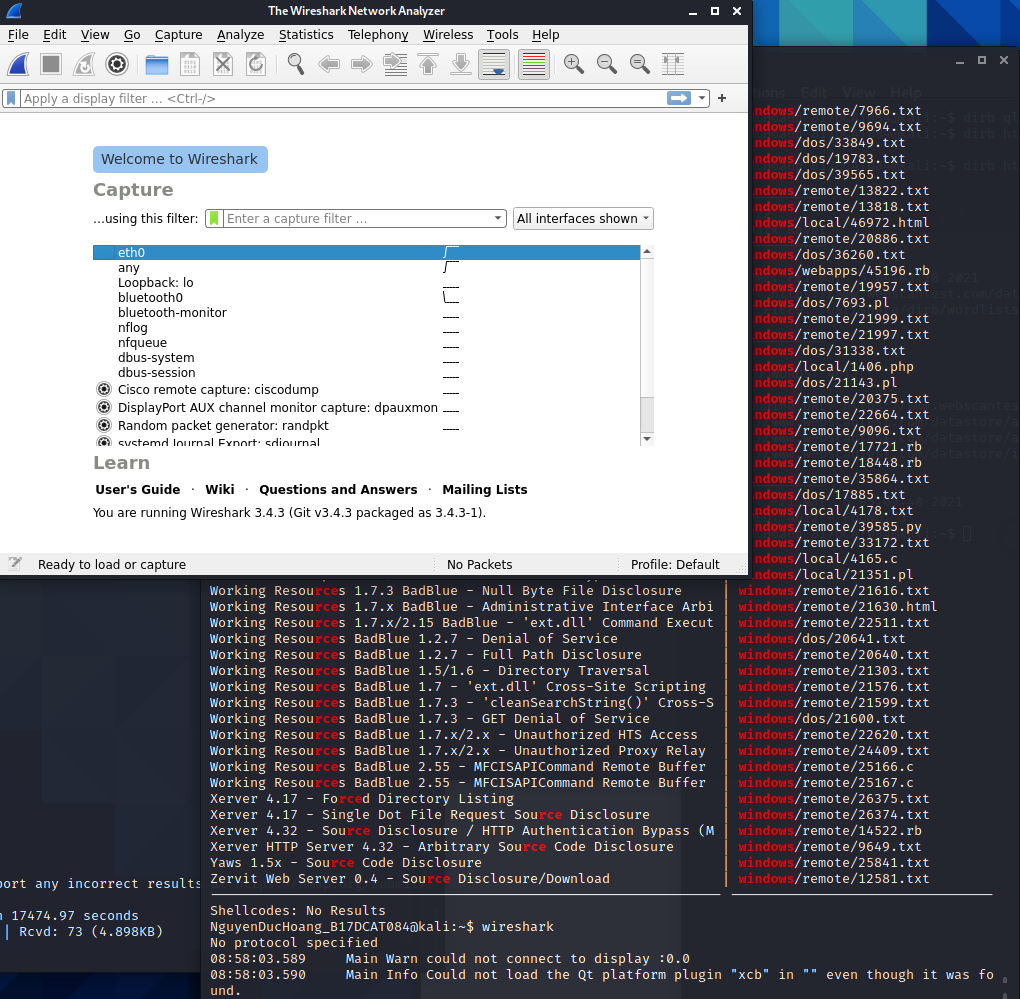
Searchsploit <keyword1> <keyword2> …



Hình : Sử dụng công cụ searchsploit tìm kiếm payload khai thác

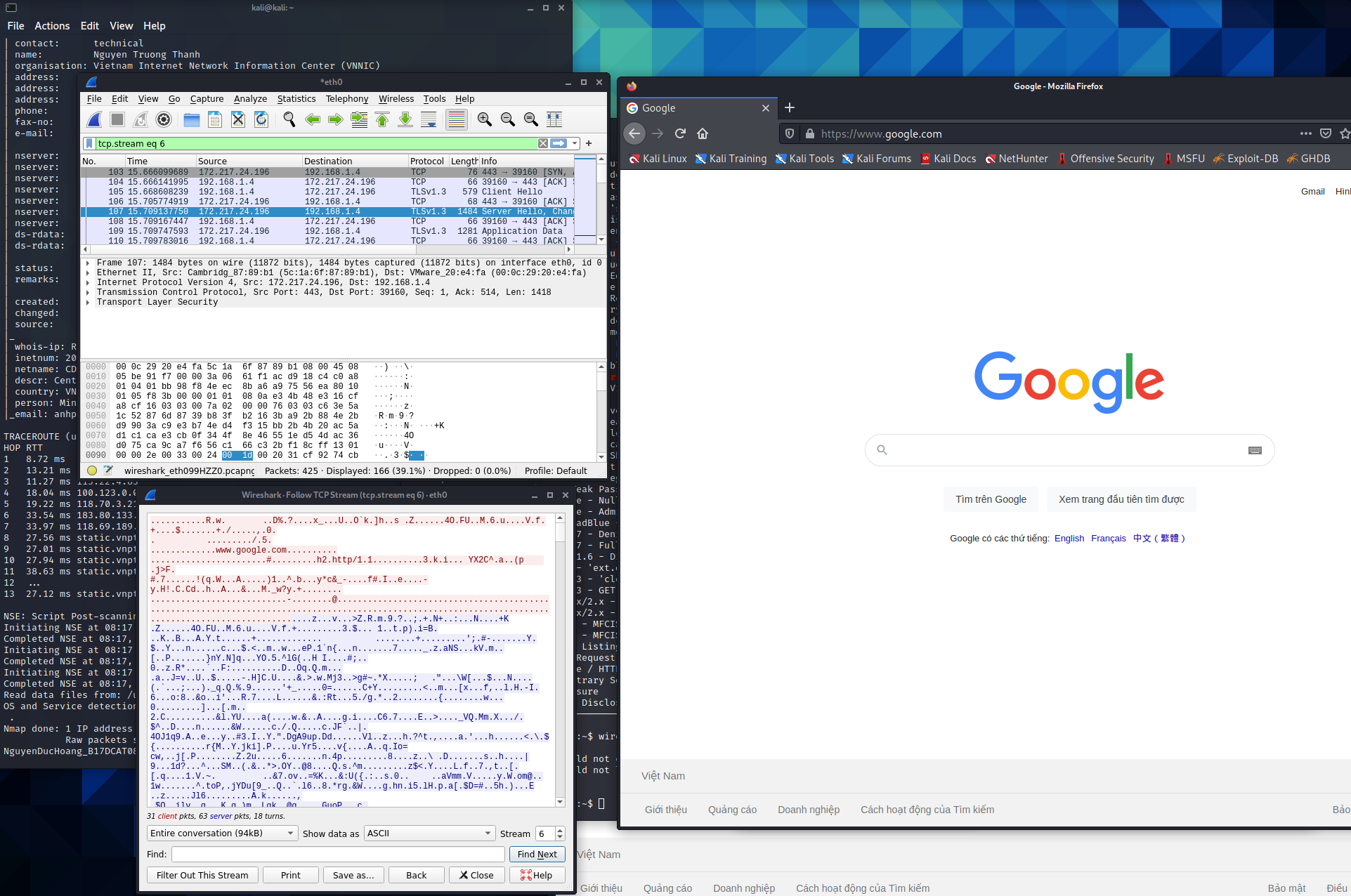
### Sniffing & Spoofing: wireshark

* Wireshark là công cụ sử dụng để bắt các gói tin ra/vào mạng trên các interface nhất định.
* Sử dụng:



Hình : Giao diện wireshark

* + Chọn interface để lắng nghe, công cụ sẽ hiển thị danh sách các gói tin vào ra theo thời gian thực.

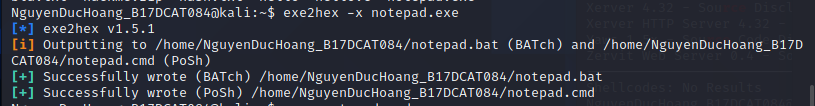


Hình : Sử dụng công cụ wireshark lắng nghe trên các interface

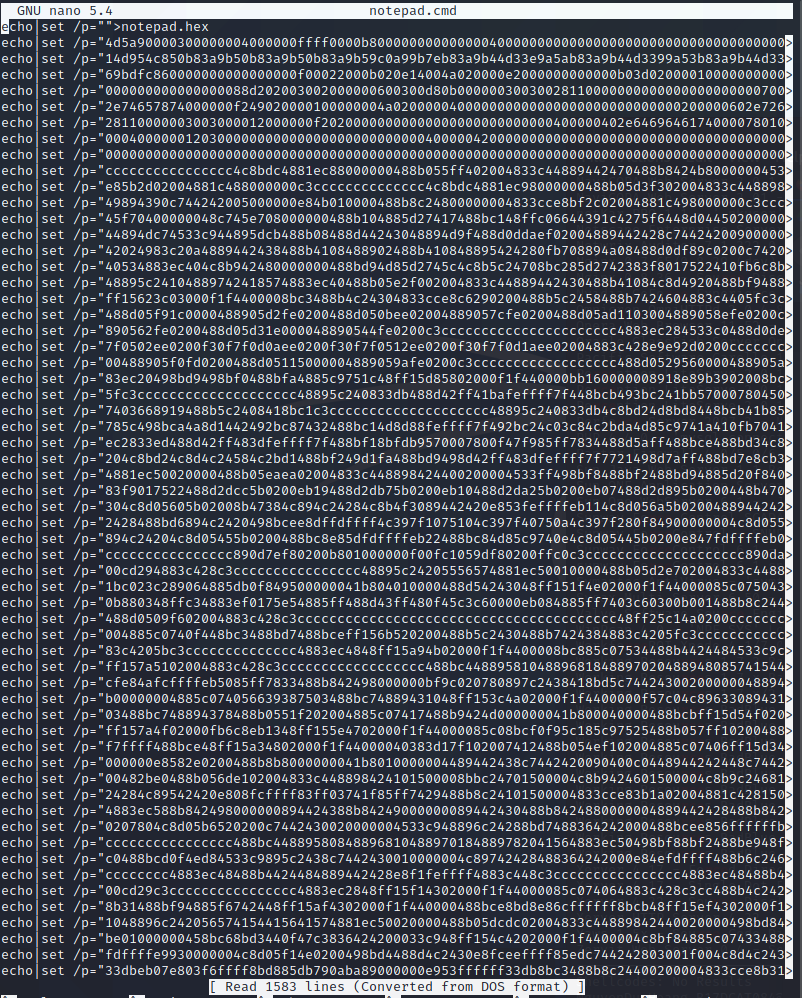
### Post Explotation: exe2hex

* Là công cụ được sử dụng để chuyển đổi file PE, bashfile,… thành dạng hex thường được sử dụng bởi mã độc trên Windows thông qua PowerShell hoặc bat/cmd file.
* Command exe2hex:

Exe2hex -x <file\_to\_convert>



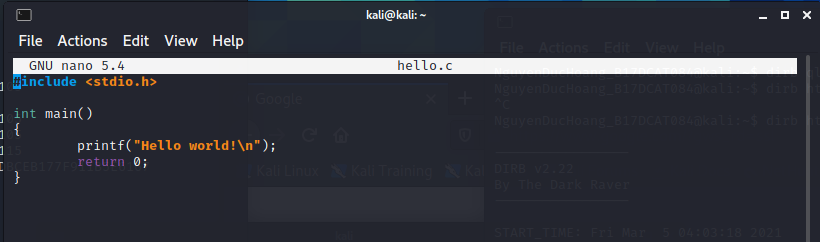
Hình : Sử dụng công cụ exe2hex



Hình : Output file của exe2hex

# Bài 2: Tìm hiểu cách lập trình C trên Linux

* Sử dụng một trình soạn thảo (vim, nano,…) để lập trình



Hình : Lập trình C trên Linux sử dụng nano

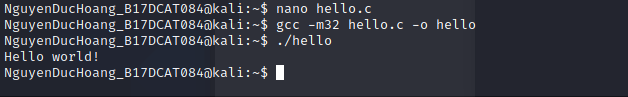
* Command biên dịch:

Gcc <file\_c> -o <output\_file>

* Lưu ý:
  + Để biên dịch chương trình x86 trên môi trường x86-64, lập trình viên sẽ cần cài đặt thêm các thư viện x86 thông qua command

apt-get install gcc-multilib và command biên dịch cần thêm option -m32

* + Một số thư viện gcc chạy trên nhân UNIX khác trên Windows.



Hình : Biên dịch và chạy chương trình C trên Linux

# Bài 3: Tìm hiểu các Command trên Linux