BÀI THỰC HÀNH SỐ 2

Môn: MẬT MÃ & AN NINH MẠNG

-o0o-

**Họ tên: Phạm Duy Quang**

**MSSV: 2011899**

**Nhóm: L01**

**1. Tìm hiểu Kali Linux và các công cụ liên quan**

- Kali Linux là gì ?

Kali Linux là một bản phân phối Linux được phát triển và duy trì bởi Offensive Security khi được tổ chức này phát hành vào tháng 3 năm 2013, là sự thay thế phát triển cho hệ điều hành BackTrack. Offensive Security là một tổ chức nổi tiếng và đáng tin cậy trong thế giới bảo mật, thậm chí chứng nhận các chuyên gia bảo mật với một số chứng chỉ được xem trọng nhất hiện có như: OSCP, OSCE, OSWP, OSEE. Kali Linux là một hệ điều hành được sử dụng nhiều trong lĩnh vực bảo mật, bởi cả những hacker tìm cách xâm nhập hệ thống và những chuyên gia về bảo mật muốn bảo vệ các tài nguyên thông tin. Kali Linux cung cấp rất nhiều công cụ cho những tác vụ liên quan đến bảo mật.

- Hãy cho biết các nhóm công cụ liên quan hiện có trên Kali Linux.

Các nhóm công cụ liên quan hiện có trên Kali Linux:

01 - Information Gathering

02 - Vulnerability Analysis

03 - Web Application Analysis

04 - Database Assessment

05 - Password Attacks

06 - Wireless Attacks

07 - Reverse Engineering

08 - Exploitation Tools

09 - Sniffing & Spoofig

10 - Post Exploitation

11 - Forensics

12 - Reporting Tools

13 - Social Engineering Tools

Graphical user interface, text

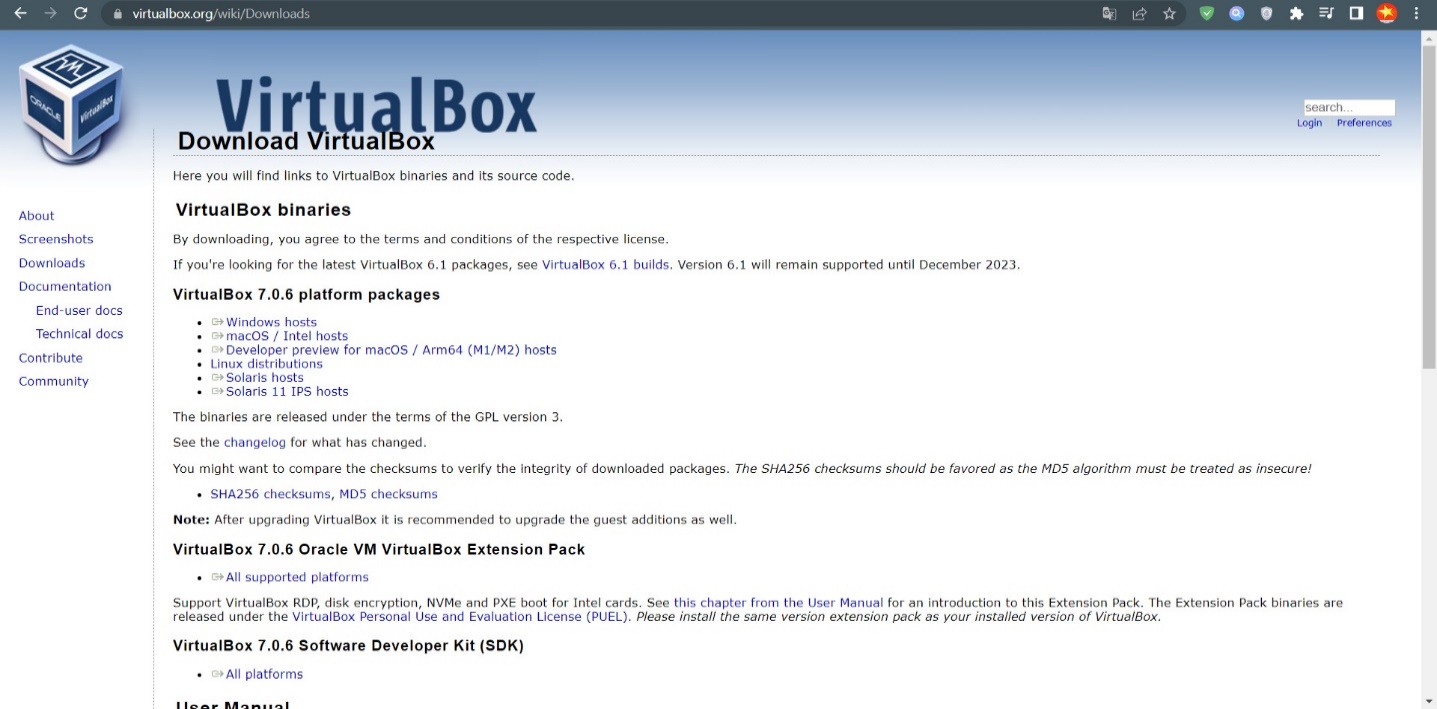
Description automatically generated

**2. Cài đặt máy ảo Kali Linux**

- Cài đặt môi trường ảo hóa (Virtual Box). Hãy cho biết các bước và một số hình ảnh:

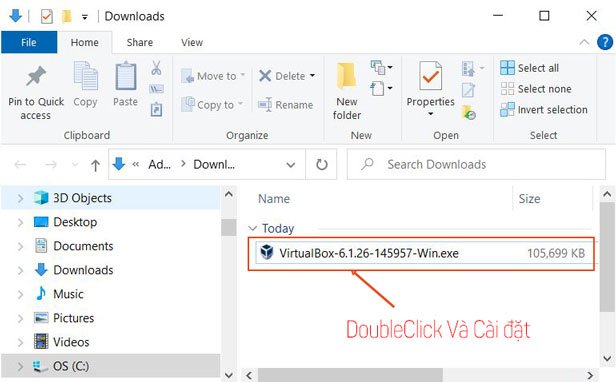
*Download VirtualBox*

Để tải VirtualBox với version mới nhất ta truy cập địa chỉ: <https://www.virtualbox.org/wiki/Downloads>.

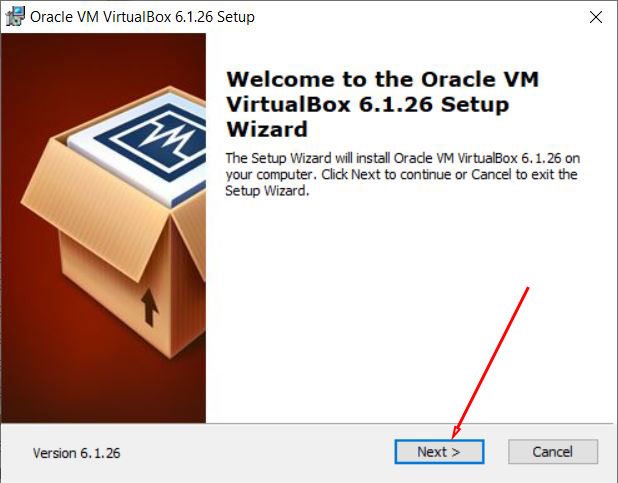


*Bắt đầu cài đặt VirtualBox*

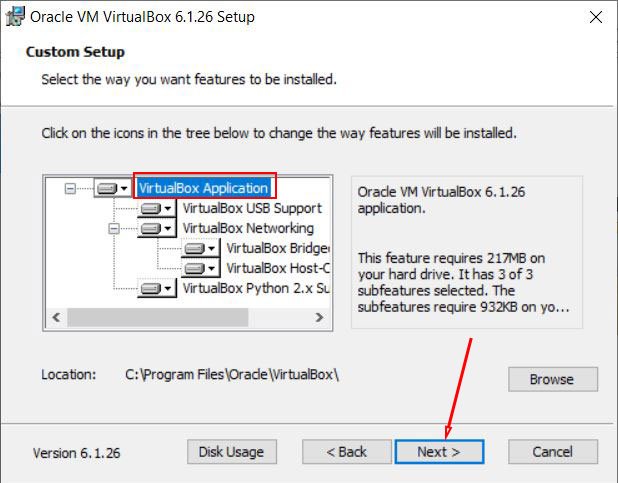
Bước 1: Sau khi tải về xong, nhấn đúp chuột để chạy file cài đặt.



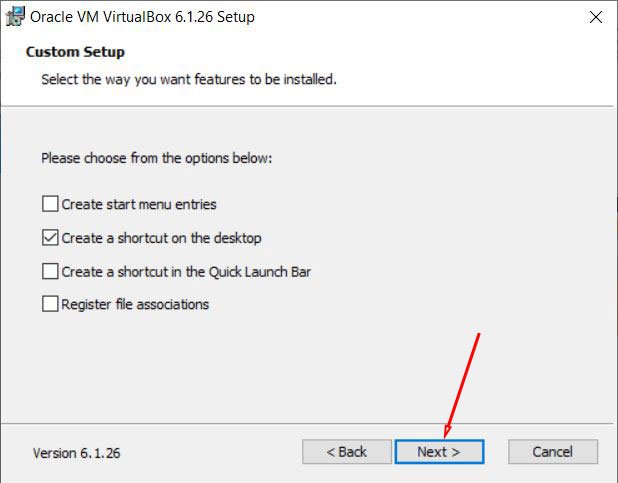
Bước 2: Nhấn Next để tiếp tục.



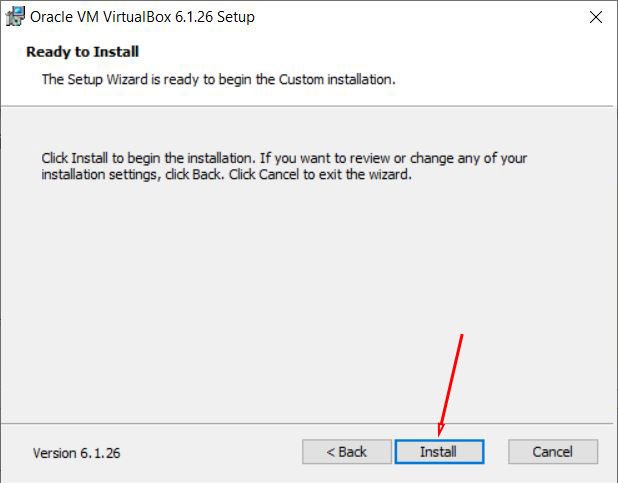
Bước 3: Tiếp tục nhấn Next như hình.



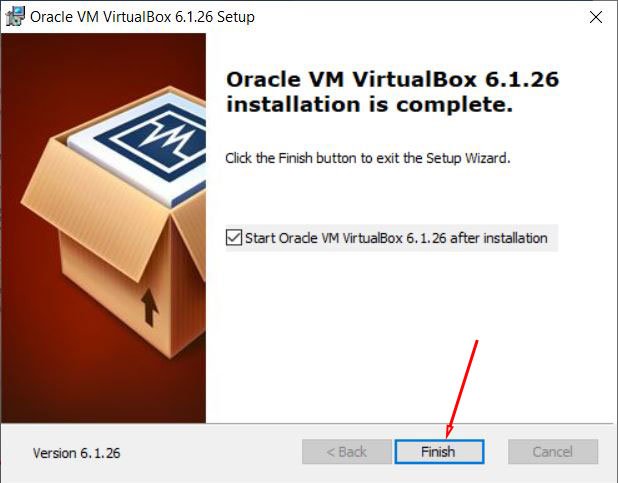
Bước 4: Chọn như hình và lại nhấn Next tiếp tục.



Bước 5: Nhấn Install để cài đặt chương trình.



Bước 6: Nhấn Finish và xác nhận thành quả.



Kết quả sau khi cài đặt thành công:



- Dowload và tạo máy ảo Kali Linux. Hãy cho biết các bước và một số hình ảnh:

Bước 1: Tải Kali Linux tại đây: <https://www.kali.org/get-kali/#kali-installer-images>.

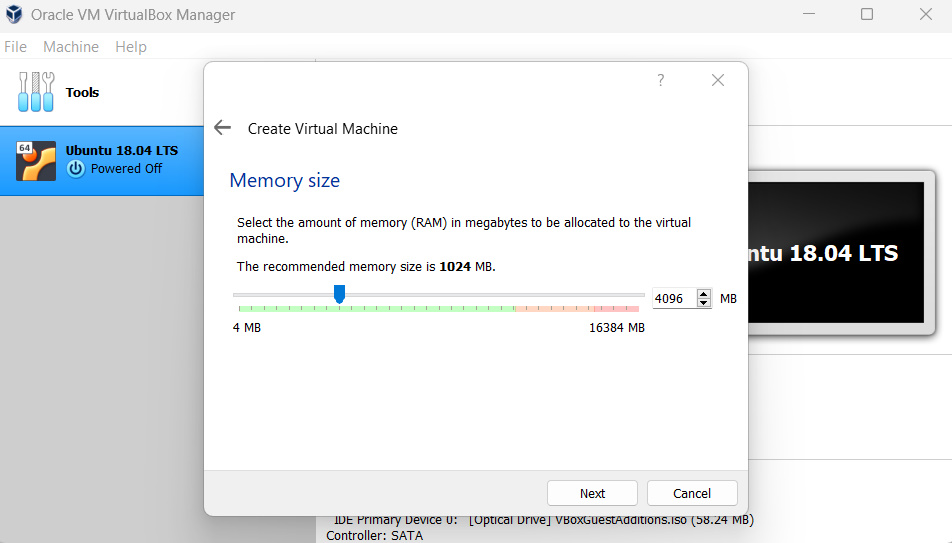
Graphical user interface, application

Description automatically generated

Bước 2: Khởi động virtual box và tạo một máy ảo (virtual machine) khách.

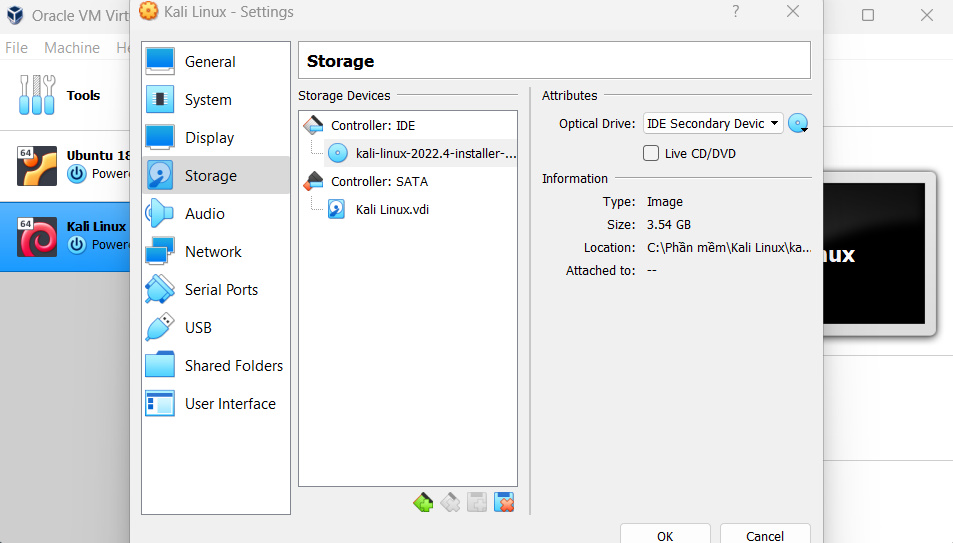
Graphical user interface, text, application

Description automatically generated



Graphical user interface, text, application

Description automatically generated



Bước 3: Ta tiến hành cài đặt Kali Linux trên Virtualbox.

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

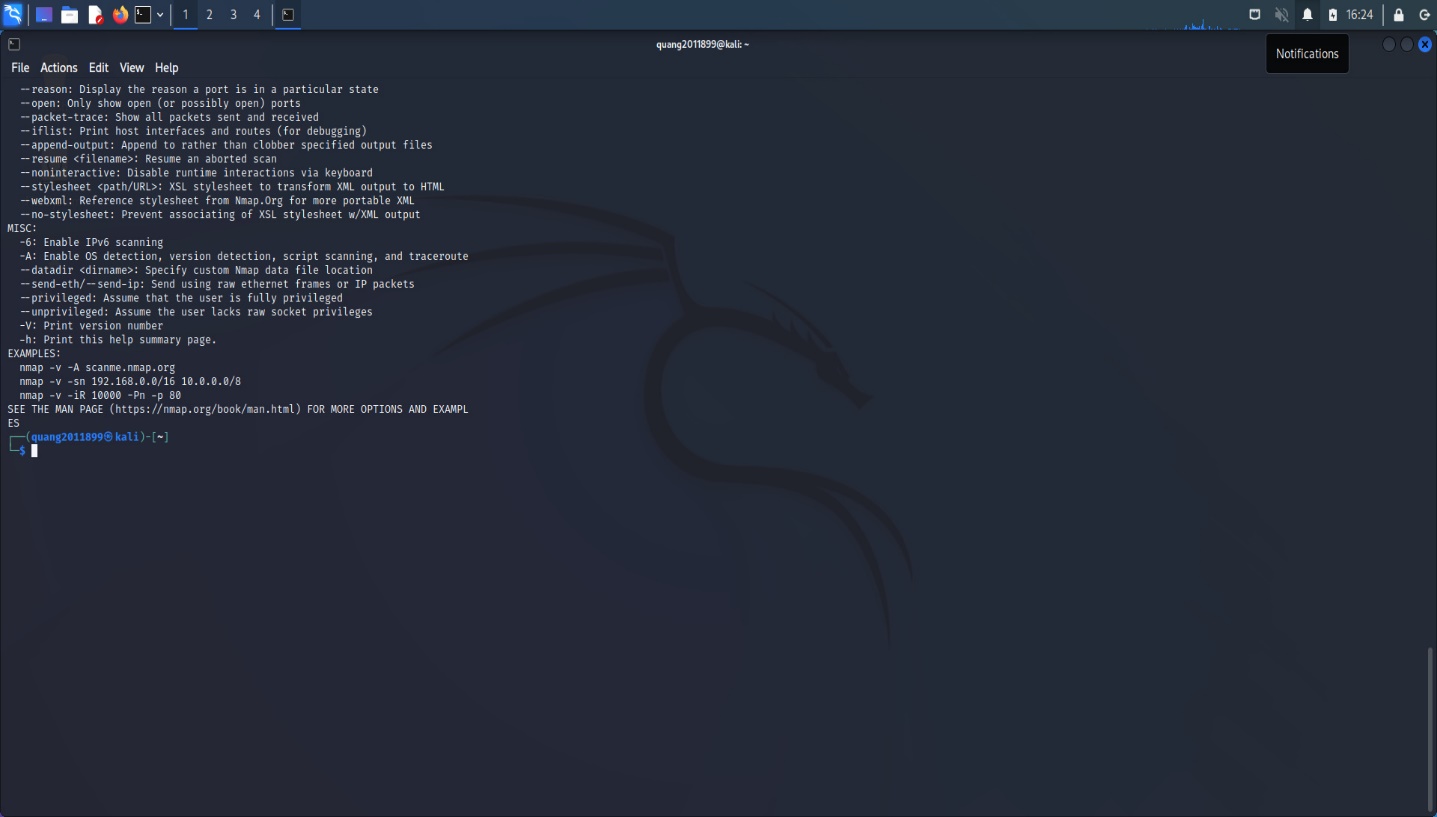
Kết quả sau khi cài đặt thành công Kali Linux trên Virtualbox:



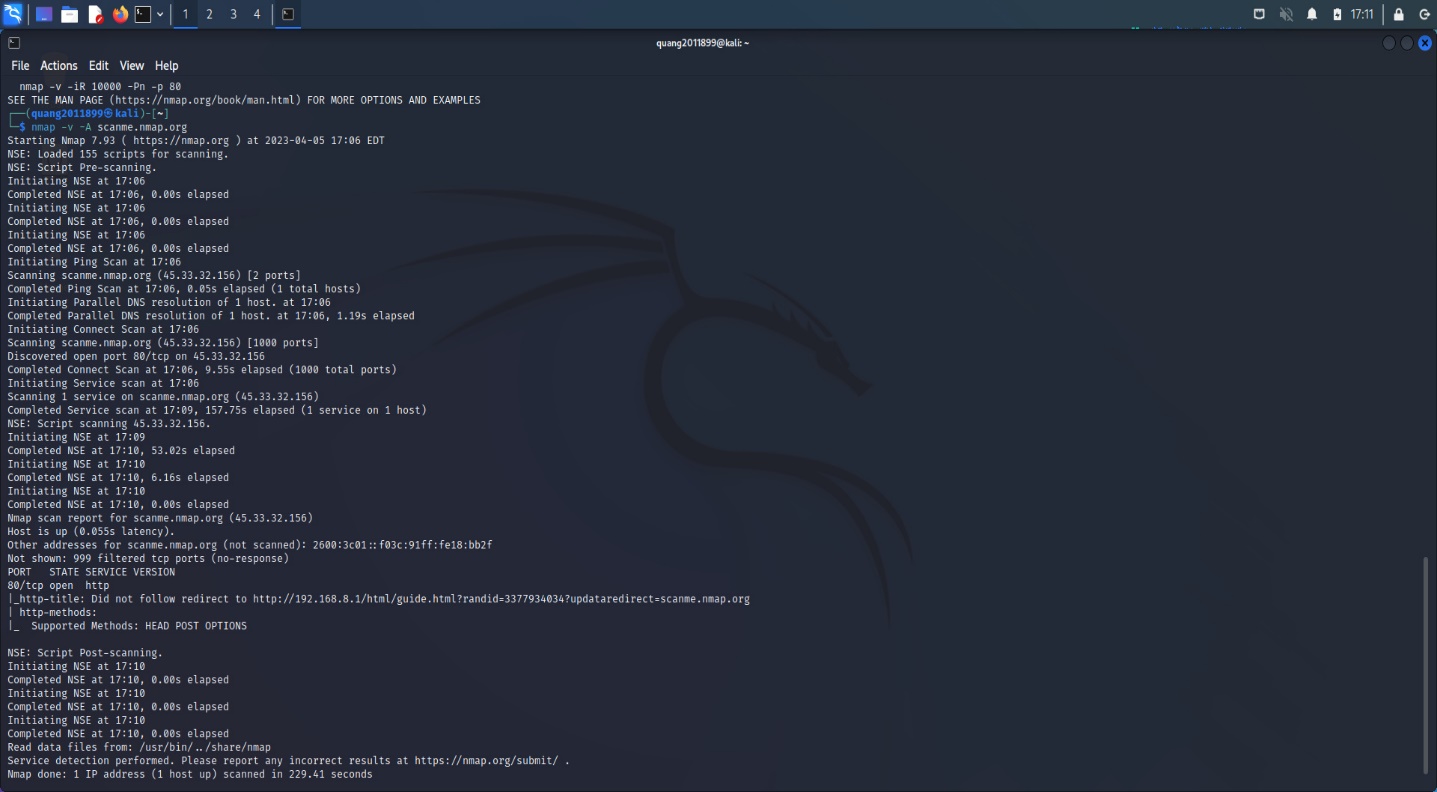
**3. Thu thập thông tin mạng bằng cách quét mạng**

- Sử dụng công cụ [Nmap](https://tools.kali.org/information-gathering/nmap)/[Zenmap](https://www.linkedin.com/pulse/gui-based-nmap-zenmap-included-kali-linux-britto-sidhan). Hãy cho biết các bước và một số hình ảnh:

+ Khởi động Nmap:



+ Nhập lệnh “nmap -v -A scanme.nmap.org”, kết quả như sau:

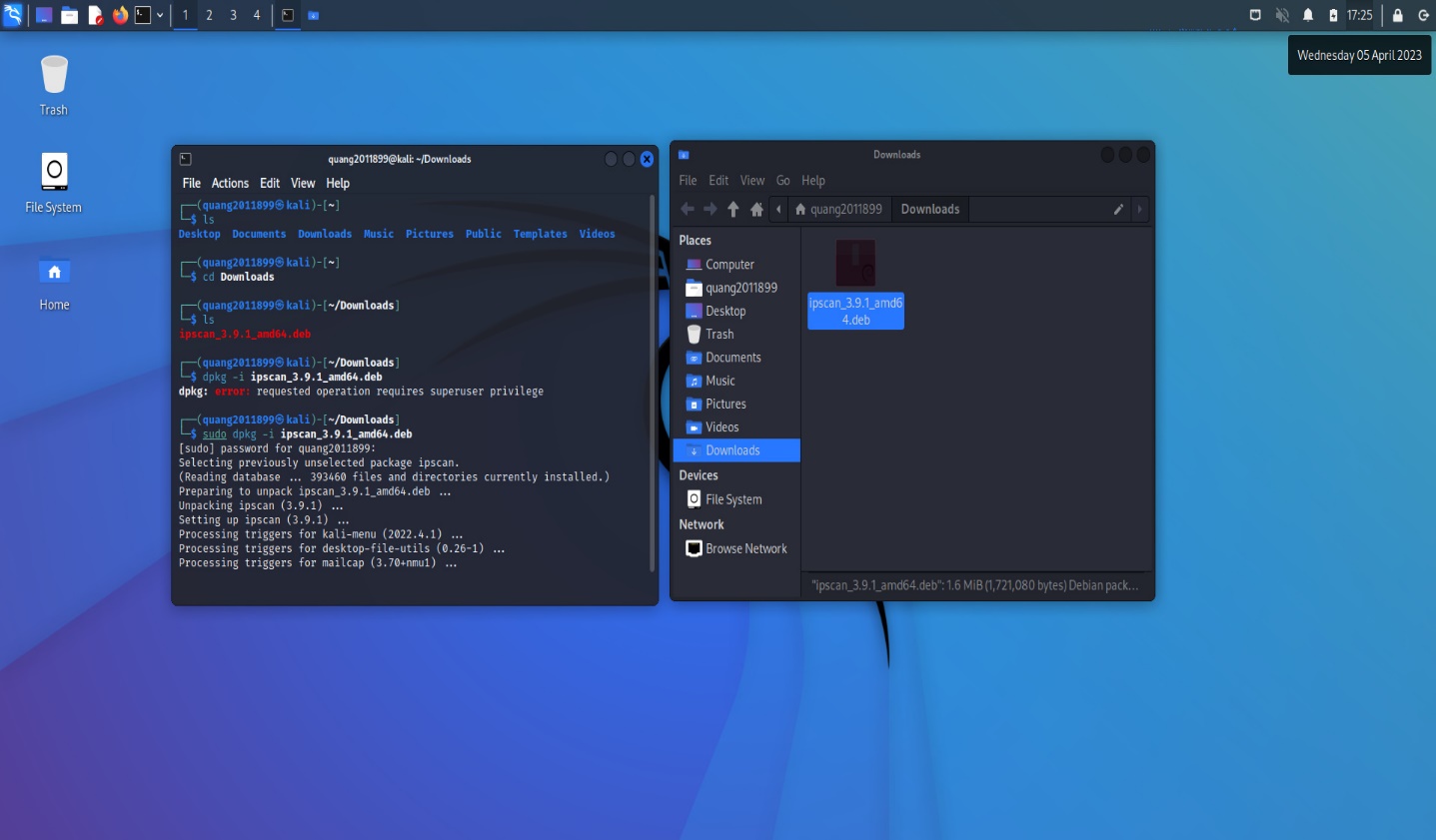


- Sử dụng [Angry IP Scanner](https://www.blackmoreops.com/2015/11/17/install-angry-ip-scanner-on-kali-linux/). Hãy cho biết các bước và một số hình ảnh:

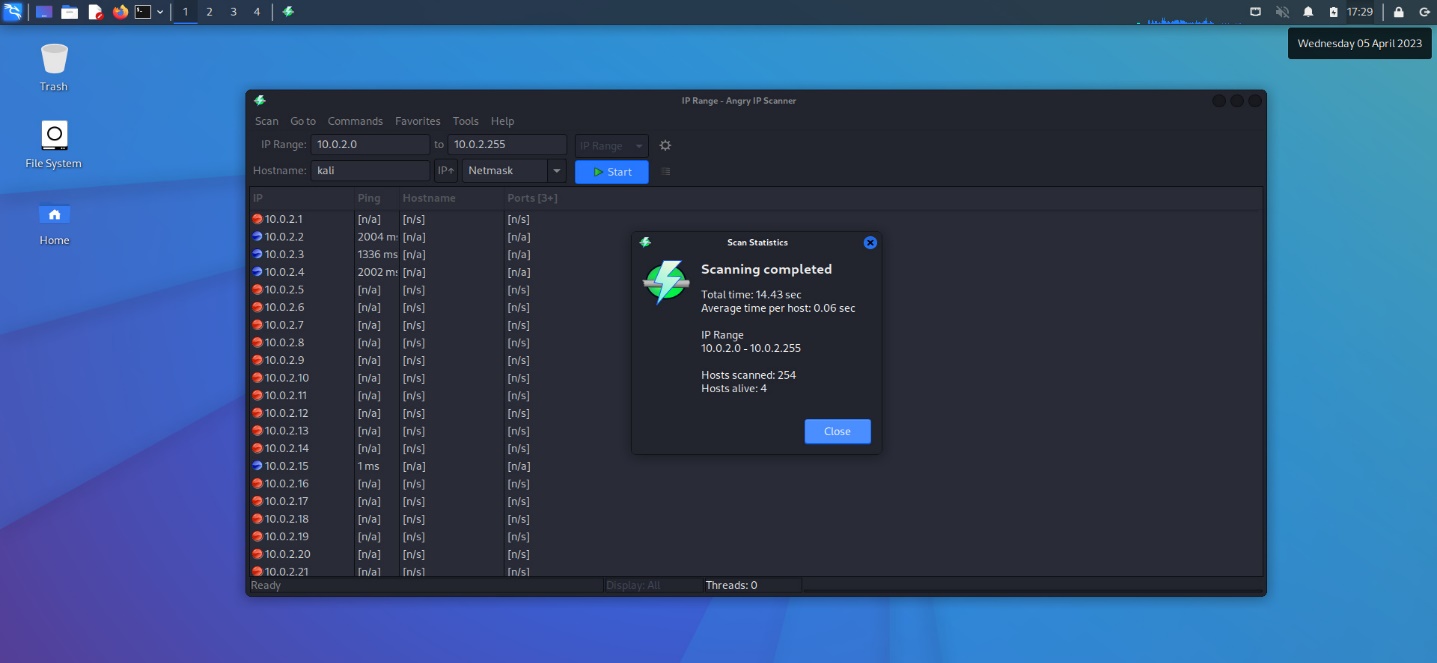
+ Cài đặt Angry IP Scanner:

Graphical user interface, website

Description automatically generated



+ Mở Angry IP Scanner và nhấn Start để bắt đầu Scan:



- Đánh giá mức độ nguy hiểm của loại hình tấn công này:

+ Tấn công thụ động.

+ Thu được các thông tin về hệ điều hành, các port đang mở, gói phần mềm.

- Biện pháp đối phó đối với loại hình tấn công là gì ?

+ Không thể dùng mã hóa.

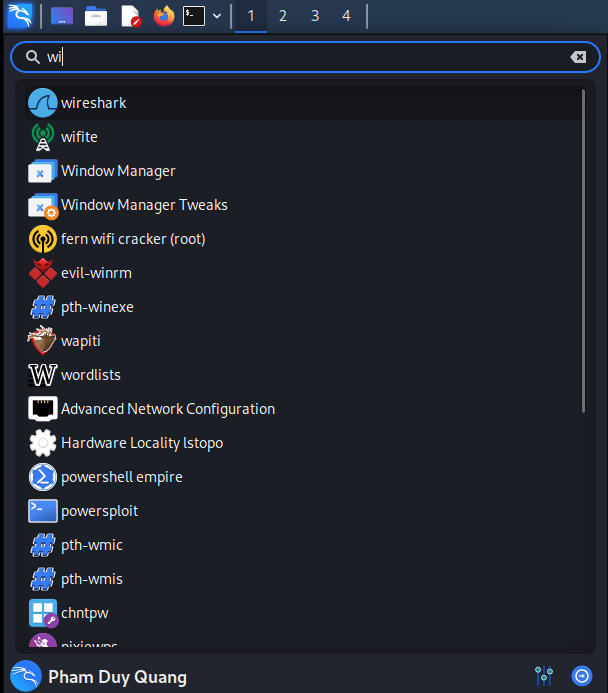
+ Phát hiện xâm nhập bất hợp pháp: Nếu dò quét mạng xảy ra thì phải chặn ngay.

+ Các hệ điều hành, phần mềm quan trọng thì phải biên dịch lại che dấu thông tin nhạy cảm (tên hệ điều hành, gói phần mềm, phiên bản,…).

**4. Nghe lén thông tin, dữ liệu**

- Dùng Wireshark để bắt gói, phân tích gói tin bắt được. Hãy cho biết các bước và một số hình ảnh:

+ Khởi động Wireshark:

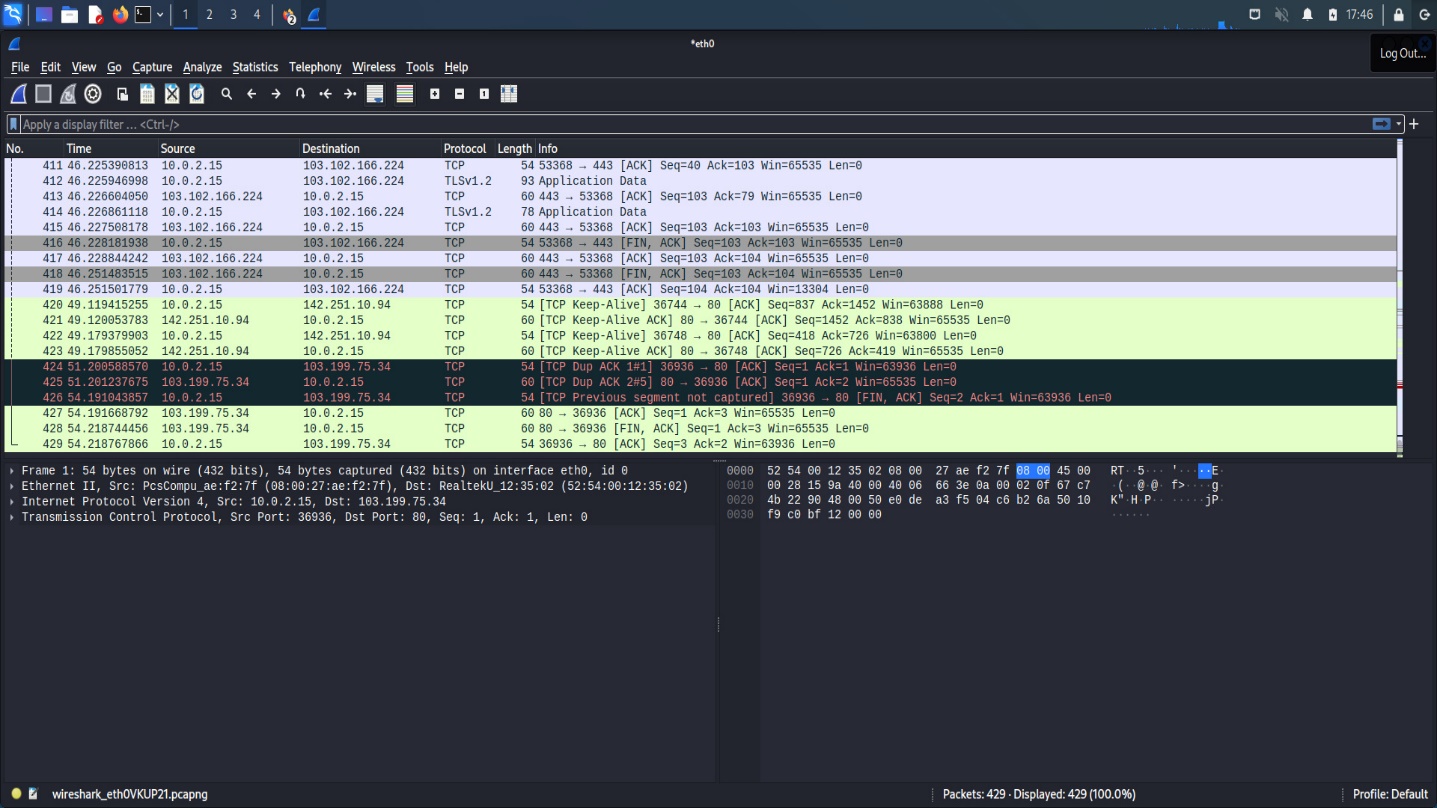


+ Chọn interface để bắt gói:

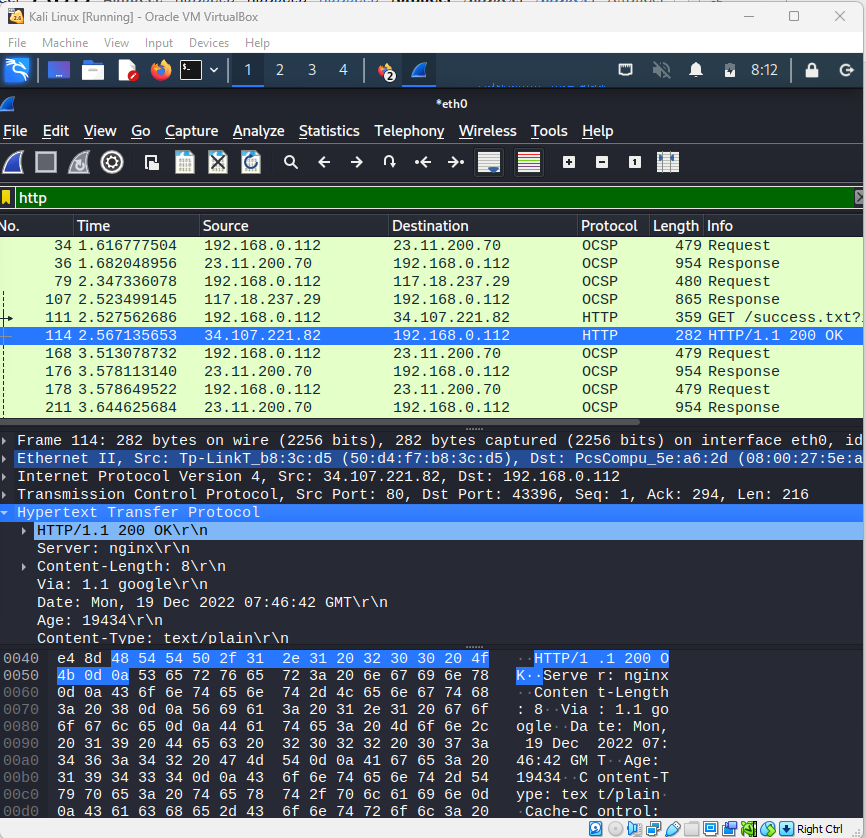
Graphical user interface, text, application

Description automatically generated

+ Nhấn “Stop capturing packets”:



+ Ta có thể inspect một gói tin bằng cách click vào nó:



- Đánh giá mức độ nguy hiểm của loại hình tấn công này:

Thu thập những thông tin nhạy cảm.

- Biện pháp đối phó đối với loại hình tấn công là gì ?

Các giao thức trên mạng: Mã hóa end – end Không thể bắt gói được.

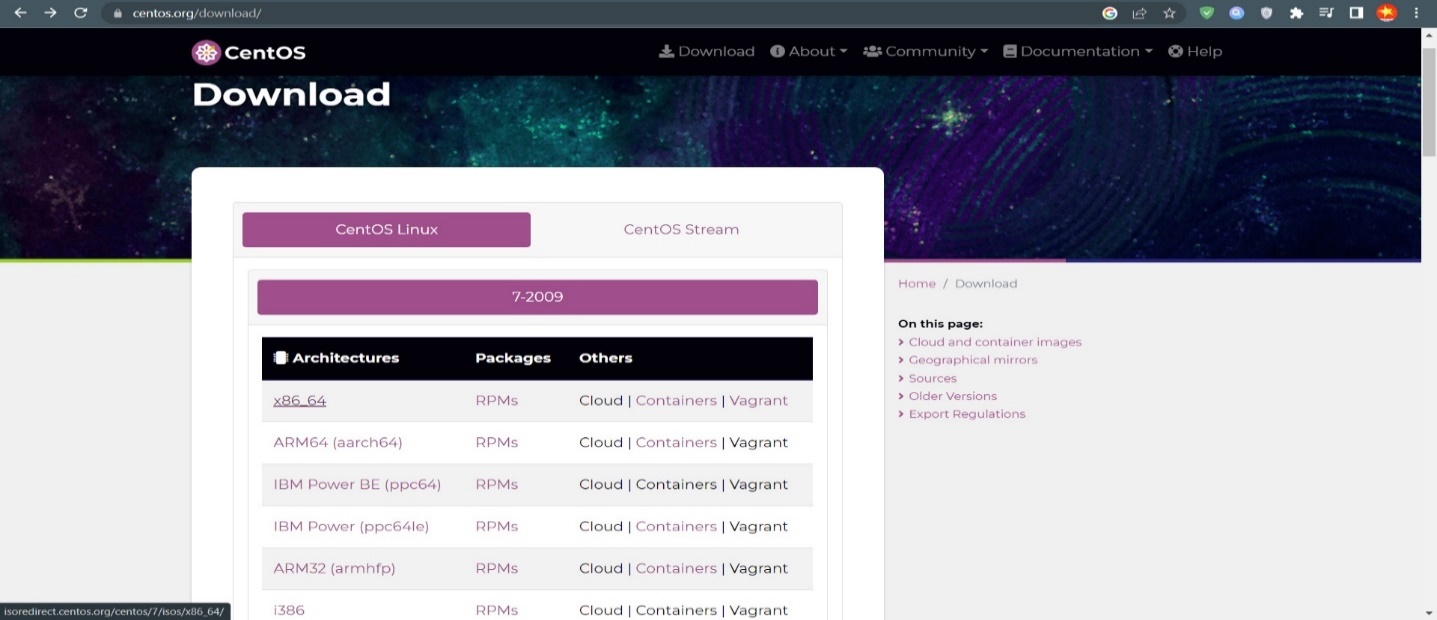
**5. Cài đặt máy chủ CentOS 7**

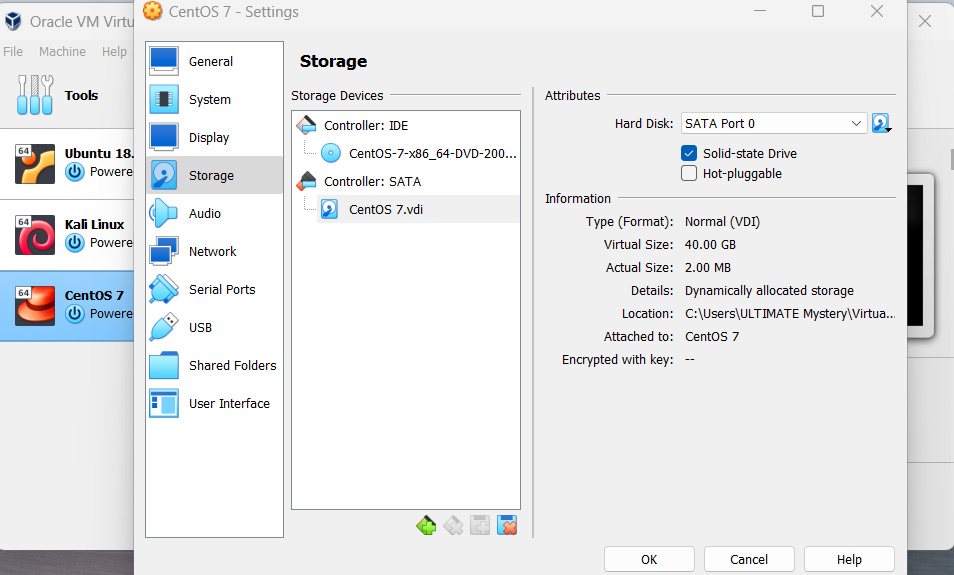
- Hệ điều hành CentOS là gì ?

CentOS là một hệ điều hành miễn phí được xây dựng và phát triển dựa trên hệ điều hành mã nguồn mở Linux. CentOS là chữ viết tắt của “Community Enterprise Operating System”. CentOS ra mắt công chúng vào tháng 5 năm 2004 và được phát triển dựa trên bản phân phối của Red Hat Enterprise Linux (RHEL).

- Hãy cho biết các bước cài đặt máy chủ CentOS 7 trên Virtual Box bao gồm vài hình ảnh.

Ta tiến hành cài đặt CentOS 7 trên Virtualbox:





Graphical user interface, application

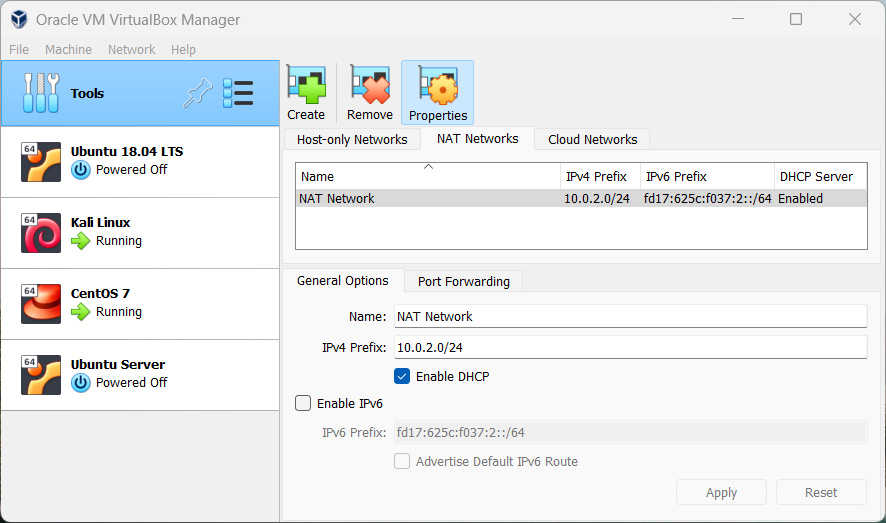
Description automatically generated

Kết quả sau khi cài đặt thành công CentOS 7 trên Virtualbox:



- Cấu hình để máy chủ CentOS và Kali Linux có thể ”thấy” nhau. Cho biết kết quả kiểm tra kết nối từ máy Kali linux đến máy chủ CentOS bằng lệnh ping:

+ Từ VirtualBox chọn Tools NAT Networks rồi tạo NAT Network như hình bên dưới:



+ Thiết lập NAT Network cho cả Kali Linux và CentOS 7:

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

+ Địa chỉ IP của máy chủ CentOS 7 là 10.0.2.6:

Text

Description automatically generated

+ Kết quả ping 10.0.2.6 từ máy Kali Linux:

A screenshot of a computer

Description automatically generated with medium confidence

**6. Tấn công vét cạn trên dịch vụ SSH của máy chủ CentOS 7**

- Tìm hiểu và cho biết cách sử dụng công cụ hydra trên Kali Linux:

Hydra là một công cụ phổ biến để khởi động các cuộc tấn công vũ phu vào thông tin đăng nhập.

Hydra có các tùy chọn để tấn công thông tin đăng nhập trên nhiều giao thức khác nhau, nhưng trong trường hợp này, chúng ta sẽ tìm hiểu về cách kiểm tra độ mạnh của mật khẩu SSH. SSH có mặt trên bất kỳ máy chủ Linux hoặc Unix nào và thường là cách chính mà quản trị viên sử dụng để truy cập và quản lý hệ thống của họ.

Để bắt đầu, hãy chọn một máy trên cùng mạng để kiểm tra. Tìm địa chỉ IP của máy đó để ta có thể chỉ cho Hydra hướng tấn công. Khi đã có IP của máy mục tiêu, hãy mở terminal trong Kali. Dùng lệnh linux sau đây để kiểm tra mật khẩu SSH của người dùng root.

$ hydra -l root -p admin 10.0.2.6 -t 4 ssh

Với -l flag sử dụng một user parameter, -p flag sử dụng một password, địa chỉ IP là địa chỉ IP của máy bị tấn công, -t là số threads sử dụng, ssh tức là Hydra sẽ tấn công SSH.

Tham khảo: <https://linuxconfig.org/ssh-password-testing-with-hydra-on-kali-linux>.

- Dùng công cụ hydra tấn công vét cạn trên dịch vụ SSH của máy chủ CentOS 7 với từ điển hiện có:

$ hydra -l root -P /usr/share/wordlists/rockyou.txt.gz 10.0.2.6 -t 4 ssh

Graphical user interface, text

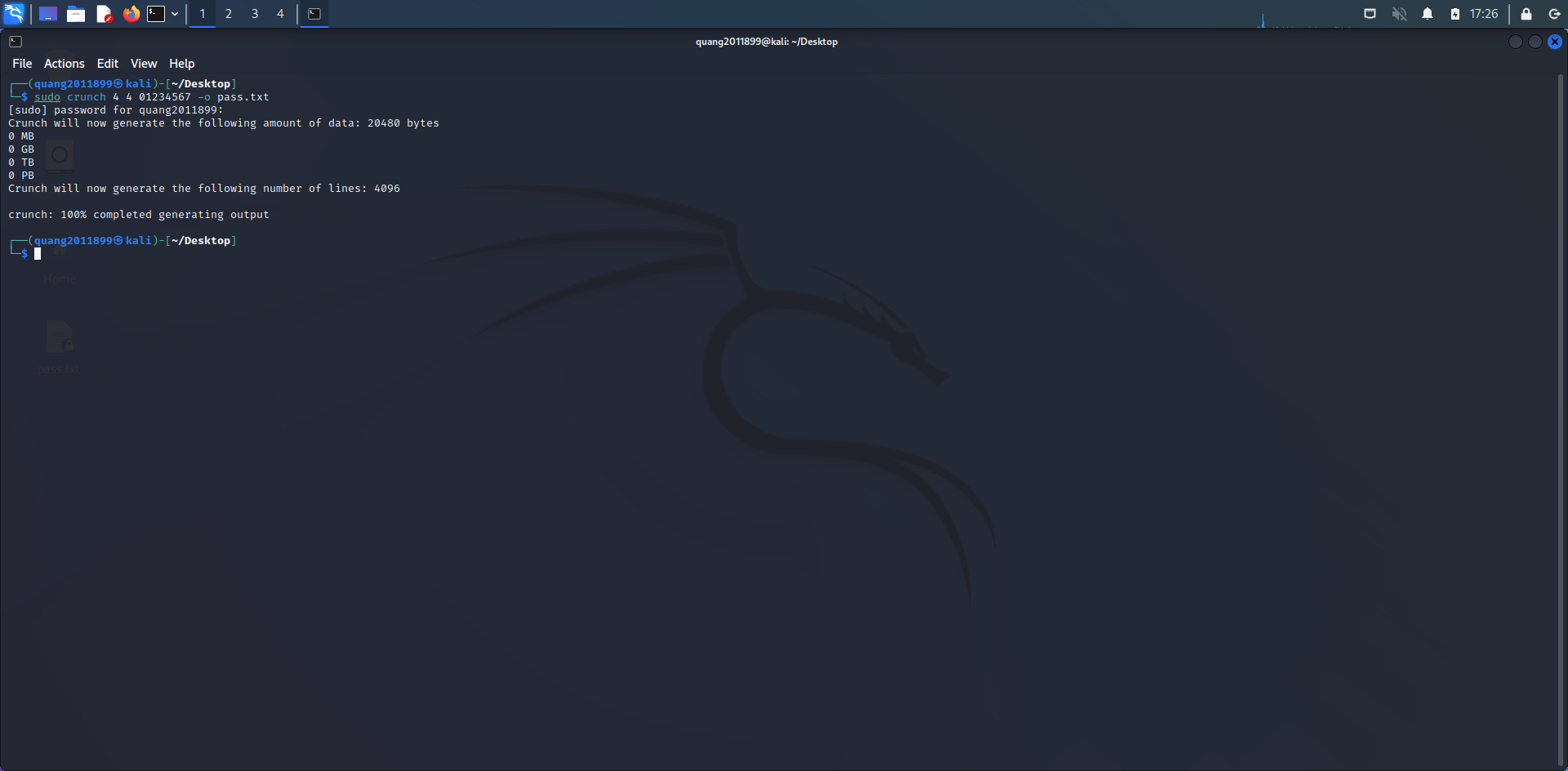
Description automatically generated

Kết quả: Ta thu được password là 12345678 ứng với user root.

- Tạo danh sách các mật khầu (wordlist) bằng crunch và dùng hydra tấn công vét cạn trên dịch vụ SSH của máy chủ CentOS 7 dùng danh sách mật khẩu đã tạo ra:

+ Tạo danh sách các mật khầu (wordlist):

$ sudo crunch 4 4 01234567 -o pass.txt



+ Thử chạy lại với wordlist mới:

$ hydra -l root -P pass.txt 10.0.2.6 -t 4 ssh

Text

Description automatically generated

- Đánh giá mức độ nguy hiểm của loại hình tấn công này:

+ Mức độ nguy hiểm lớn.

+ Có thể mất thời gian nhưng nếu có được mật khẩu của người quản trị thì có thể sử dụng để chiếm quyền quản trị (admin).

**7. Giải pháp giảm thiểu tấn công vét cạn**

- Tìm hiểu fail2ban và cho biết nó được sử dụng để làm gì ?

Fail2ban là 1 chương trình được viết bằng Python có nhiệm vụ chặn các ip kết nối đến server dựa vào các dấu hiệu nghi ngờ mà ip đó để lại trong file log của hệ thống hoặc dịch vụ. Ví dụ như có quá nhiều lần sử dụng mật khẩu không hợp lệ, truy cập không hợp lệ hoặc các dấu hiệu bất thường khác mà có thể nhận biết được. Ta có thể cài đặt fail2ban trên CentoOS 7 cấu hình chống bruteforce attack cho SSH và WordPress.

Tham khảo: <https://cuongquach.com/cai-dat-fail2ban-bao-ve-ssh-centos.html>.

- Cài đặt và cấu hình fail2ban đối với dịch vụ SSH trên máy chủ CentOS 7:

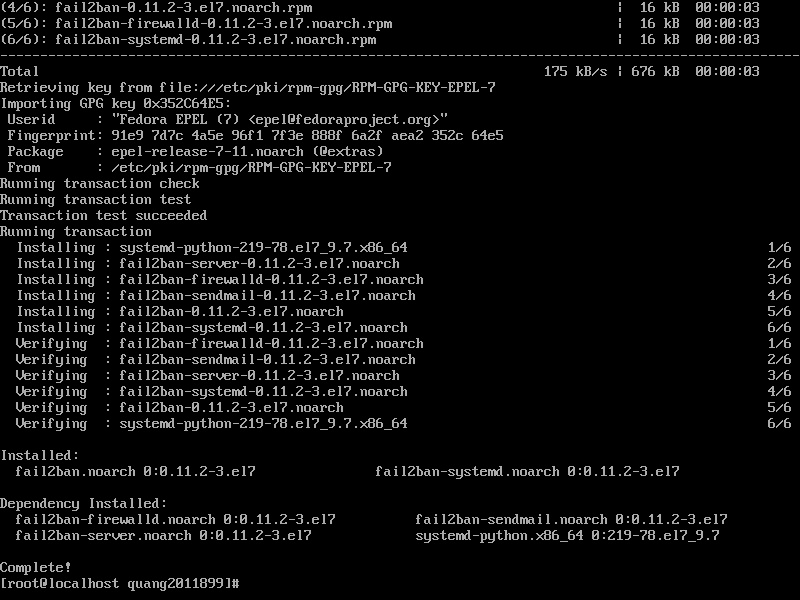
+ Cài đặt Fail2ban trên CentOS 7:

# yum -y install epel-release

Text

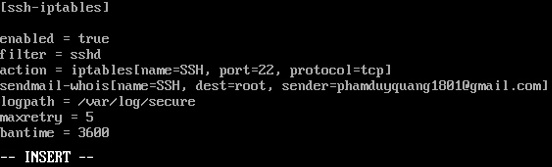
Description automatically generated

# yum -y install fail2ban fail2ban-systemd



+ Tạo file cấu hình với nội dung chỉ định cho việc bảo vệ dịch vụ SSH trên VPS/Cloud Server:

# vi /etc/fail2ban/jail.local



Giải thích cấu hình:

* enabled: kích hoạt chức năng cho phép Fail2ban bảo vệ dịch vụ được cấu hình trong section *[ssh-iptables]*. Ta có thể tắt phần cấu hình 1 section bằng giá trị “false”.
* filter: ta có thể tìm thấy tên của các mẫu file quy chuẩn hoạt động filter riêng của Fail2ban được cấu hình sẵn trong thư mục ‘/etc/fail2ban/filter.d/\*’. Ta sử dụng tên ‘ssh’, vì nó là alias name tương ứng file ‘/etc/fail2ban/filter.d/sshd.conf’, nếu file này không tồn tại thì hoạt động bảo vệ port SSH sẽ không hoạt động.
* action:
* fail2ban sẽ chặn địa chỉ IP nếu thông tin lọc khớp với khuôn mẫu trong file ‘/etc/fail2ban/filter.d/sshd.conf’, các hành vi chặn địa chỉ IP được quy định tại ‘/etc/fail2ban/action.d/iptables.conf’.
* Nếu sử dụng một port khác cho dịch vụ SSH lắng nghe trên server thì ta có thể phải chỉ định lại thông tin ‘port=<port\_number>’ trong phần cấu hình.
* Nếu ta có địa chỉ mail, thì Fail2ban sẽ gửi email đến khi địa chỉ IP bị ban. Cũng nên lưu ý, việc gửi mail thành công hay không phụ thuộc nhiều vào dịch vụ MTA mặc định của hệ thống.
* logpath: đường dẫn file log Fail2ban sử dụng để lọc liên tục các thông báo đăng nhập sai.
* maxretry: số lần login thất bại tối đa cho phép.
* bantime: thời gian khoá truy cập từ IP đăng nhập sai quá số lần ‘maxretry’. Ở đây: 3600 giây = 1 giờ.

Ta có thể thay đổi các giá trị theo mong muốn.

+ Tiến hành khởi động dịch vụ Fail2ban:

# systemctl start fail2ban

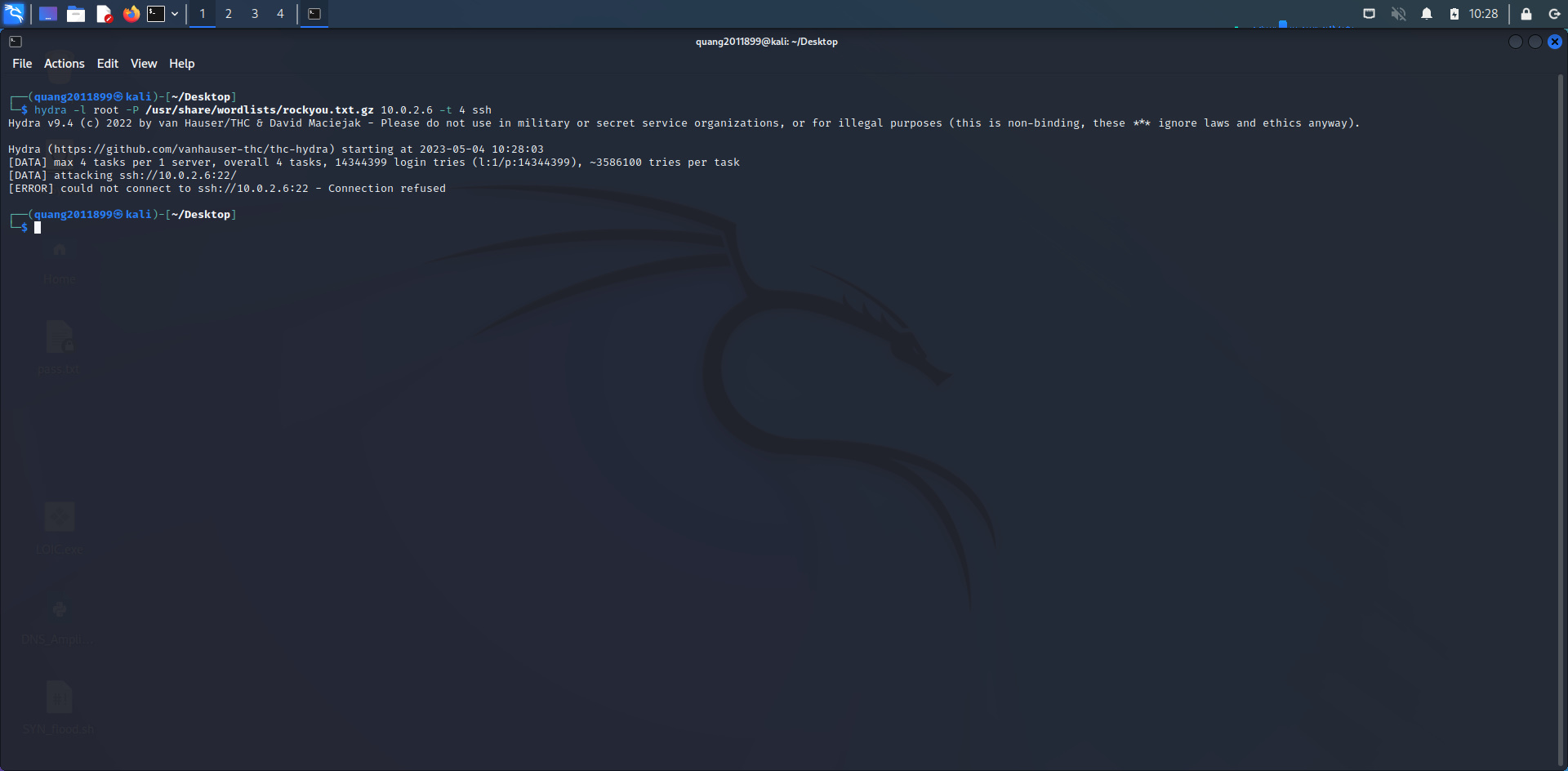
# systemctl enable fail2ban



- Dùng công cụ hydra tấn công vét cạn trên dịch vụ SSH của máy chủ CentOS 7 và cho biết kết quả:

+ Dùng công cụ hydra tấn công vét cạn trên dịch vụ SSH của máy chủ CentOS 7 với từ điển hiện có:

$ hydra -l root -P /usr/share/wordlists/rockyou.txt.gz 10.0.2.6 -t 4 ssh



Kết quả: Địa chỉ IP của máy tấn công đã bị chặn bởi Fail2ban bên máy chủ CentOS 7 do đã nhập sai mật khẩu quá nhiều lần quy định.

+ Tại máy chủ CentOS 7, lệnh dưới hiển thị hiện đang có 1 địa chỉ IP bị chặn, chính là địa chỉ IP của máy Kali Linux đã tấn công vét cạn (brute force attack) tới máy chủ CentOS 7:

# fail2ban-client status ssh-iptables

Text

Description automatically generated