BÀI THỰC HÀNH SỐ 5

Môn: MẬT MÃ & AN NINH MẠNG

**-o0o-**

Họ tên: Nguyễn Long Kim

MSSV: 1812742

**Nhóm: L06**

* + - * 1. Tìm hiểu Kali Linux và các công cụ liên quan
* **Kali Linux là gì ?**

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**

**+** Information Gathering

**+** Vulnerability Analysis

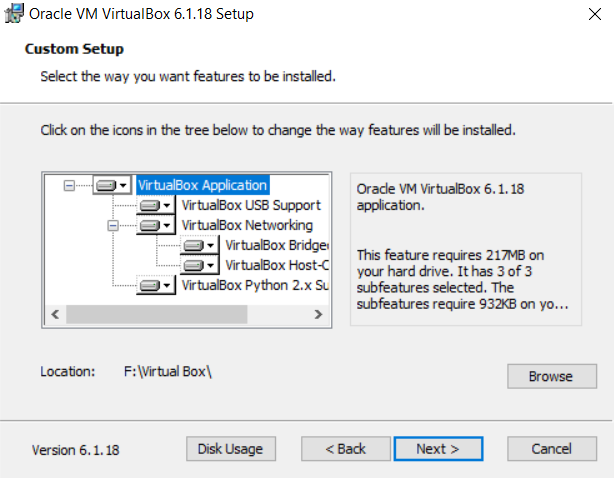
**+** Password Attack

**+** Wireless Attack

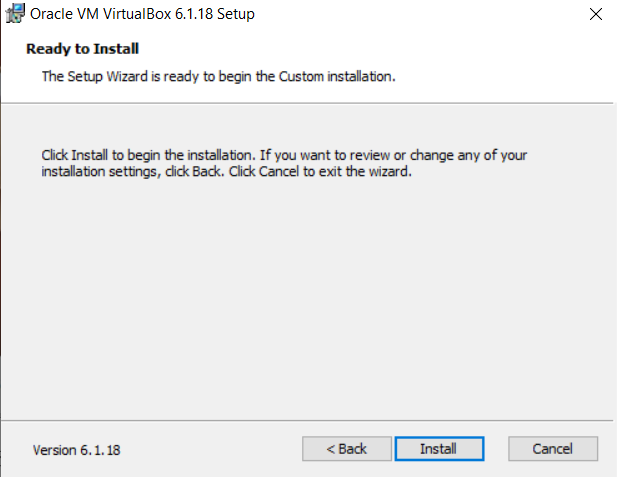
**+** Sniffing

* + - * 1. Cài đặt máy ảo Kali Linux
* **Cài đặt môi trường ảo hóa (Virtual Box). Hãy cho biết các bước và một số hình ảnh:**



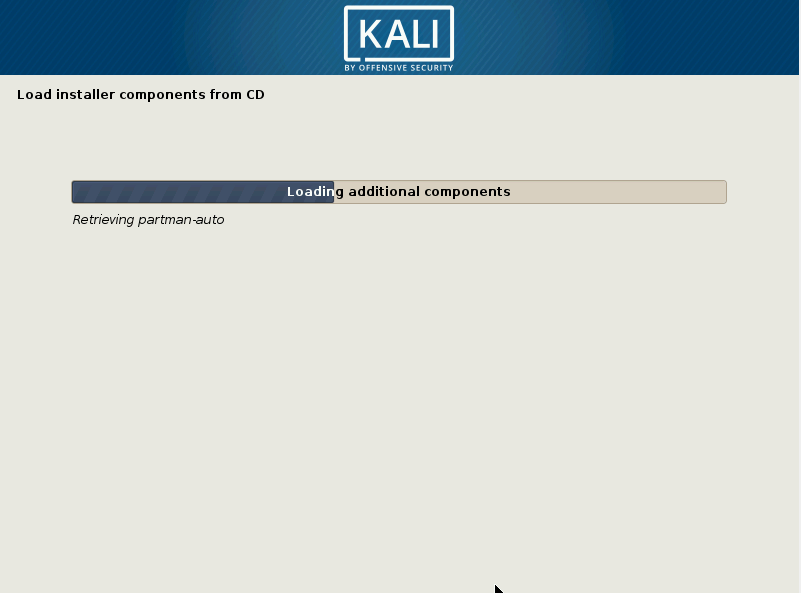


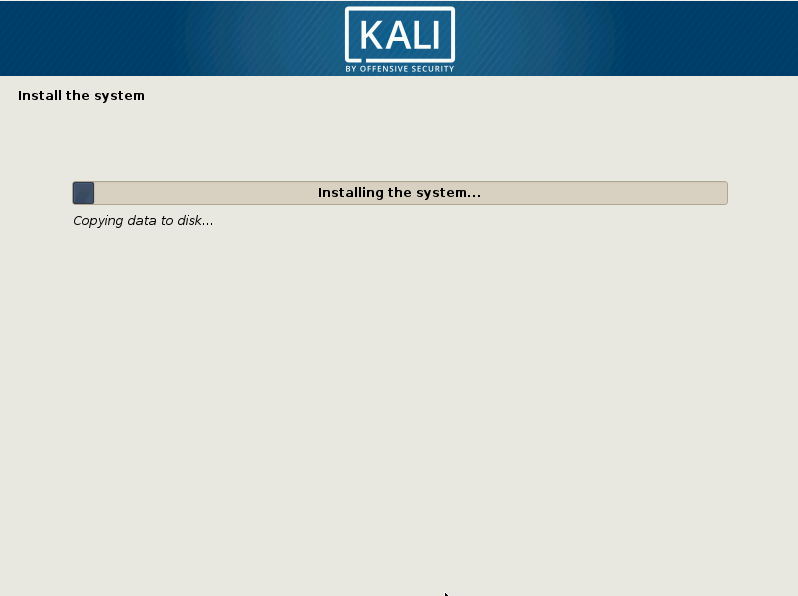




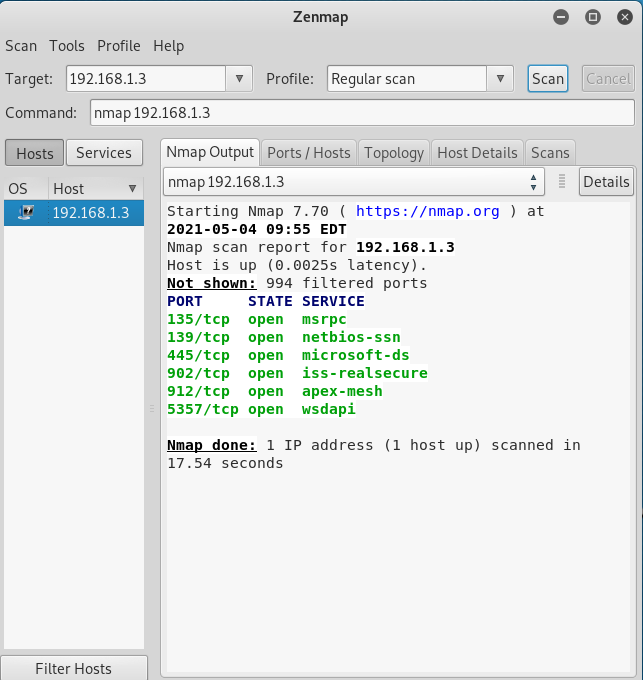
* **Dowload và tạo máy ảo Kali Linux. Hãy cho biết các bước và một số hình ảnh:**

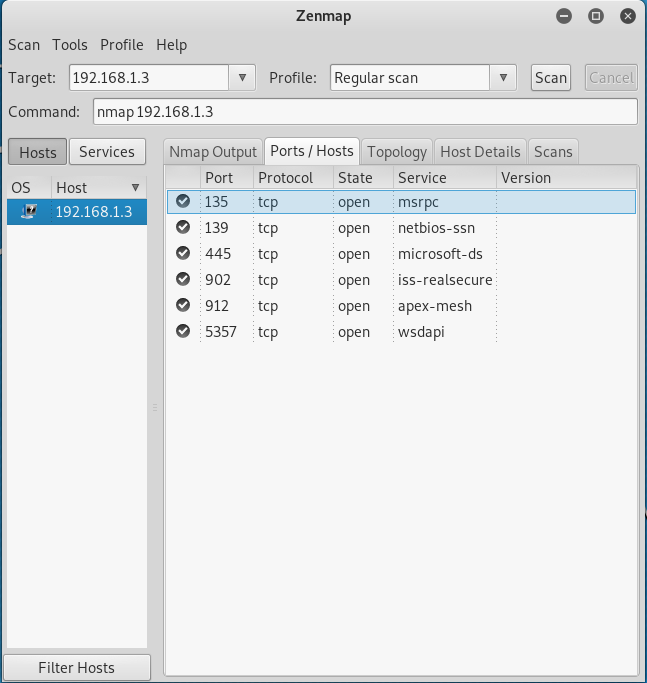






* + - * 1. Thu thập thông tin mạng bằng cách quét mạng
* **Sử dụng công cụ** [**Nmap**](https://tools.kali.org/information-gathering/nmap)**/**[**Zenmap**](https://www.linkedin.com/pulse/gui-based-nmap-zenmap-included-kali-linux-britto-sidhan)**. Hãy cho biết các bước và một số hình ảnh:**

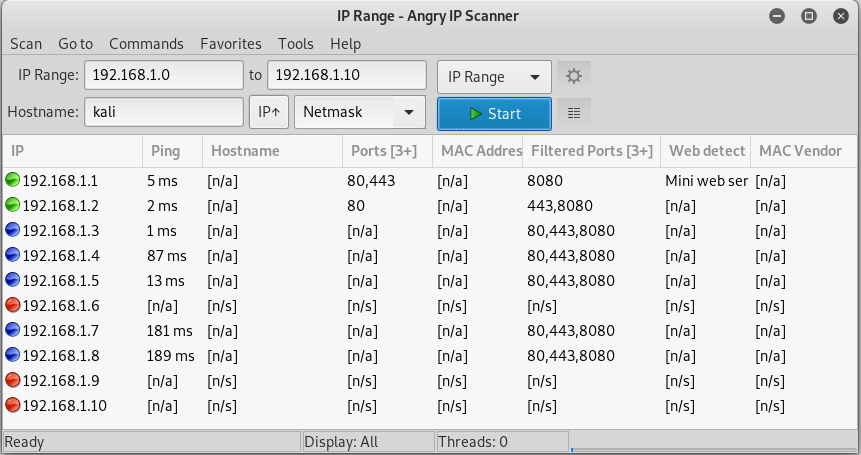






* **Sử dụng** [**Angry IP Scanner**](https://www.blackmoreops.com/2015/11/17/install-angry-ip-scanner-on-kali-linux/)**. Hãy cho biết các bước và một số hình ảnh:**





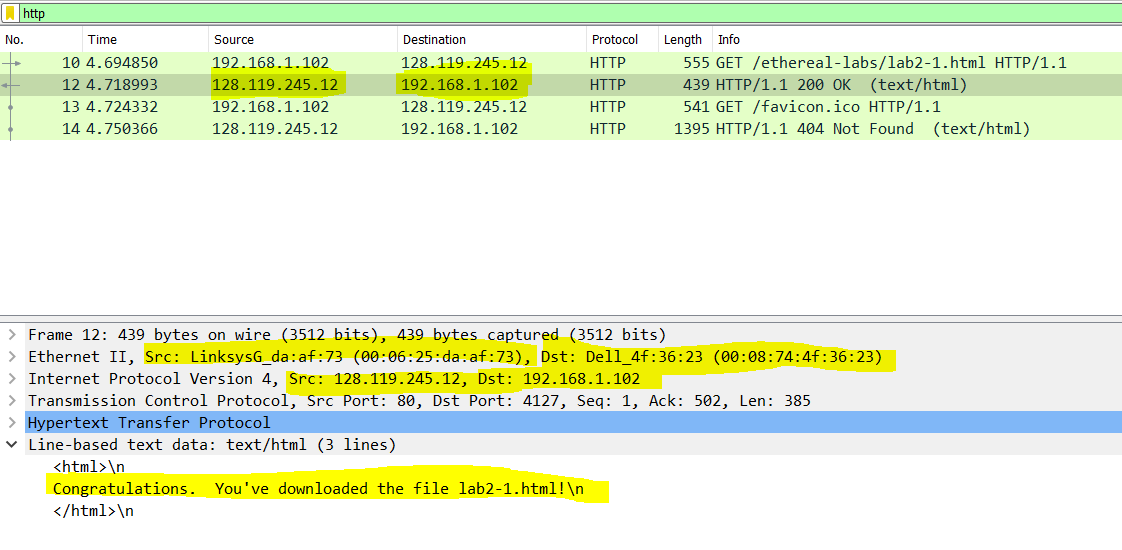
* **Đánh giá mức độ nguy hiểm của loại hình tấn công này:**

Loại hình tấn công nay có thể biết được thông tin chi tiết của các thiết bị trong mạng như địa chỉ ip, các port đang mở và dịch vụ tương ứng, hệ điều hành đang chạy trên thiết bị,… Từ đó việc tấn công sẽ dễ dàng hơn với thông tin đã biết.

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

Tìm cách để ẩn thông tin trên mạng của thiết bị khỏi “external scanner”. Một cách có thể áp dụng đó là dùng NAT device (hay firewall) cho phép thiết bị sử dụng “private address” ở trong mạng, và “public address” ở ngoài mạng.

* + - * 1. 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:**



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

Biện pháp tấn công này có thể nghe lén dữ liệu

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

Để đối phó thì chúng ta cần mã hóa dữ liệu trước khi gửi

* + - * 1. 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)**

Hệ điều hành này được tạo ra với mục đích chính là xây dựng nền tảng hệ thống máy chủ miễn phí dành cho doanh nghiệp và duy trì khả năng tương thích nhị phân với **RHEL**. Ngoài ra, **CentOS** còn cung cấp một môi trường hoàn hảo để thực hiện các công việc liên quan đến lập trình.

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

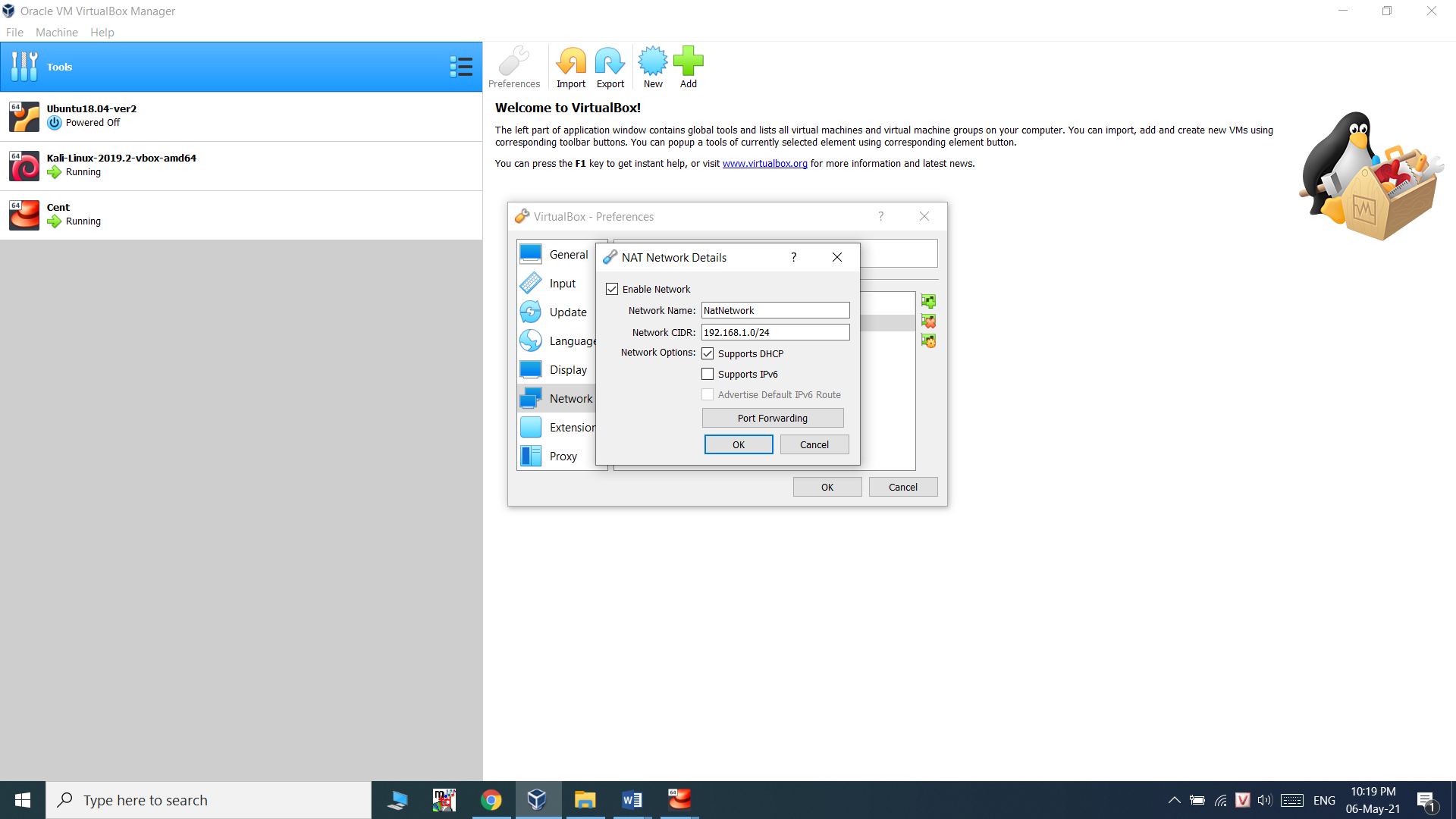


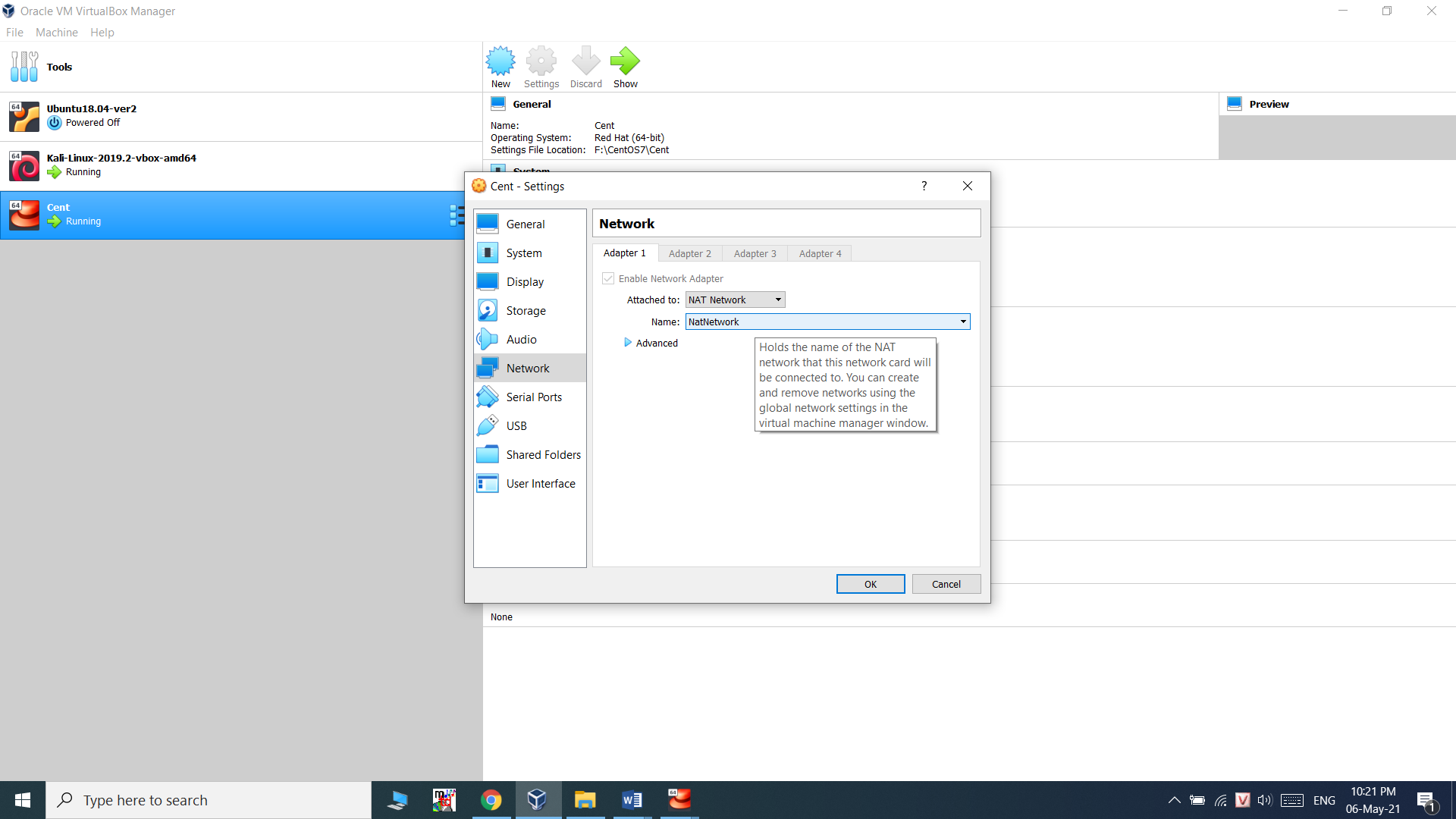
* **Cấu hình để máy chủ CentOS và Kali Linux có thể ”thấy” nhau. Cho biết kết quả kiểm tra kết nối từ máy Kali linux đến máy chủ CentOS bằng lệnh ping:**

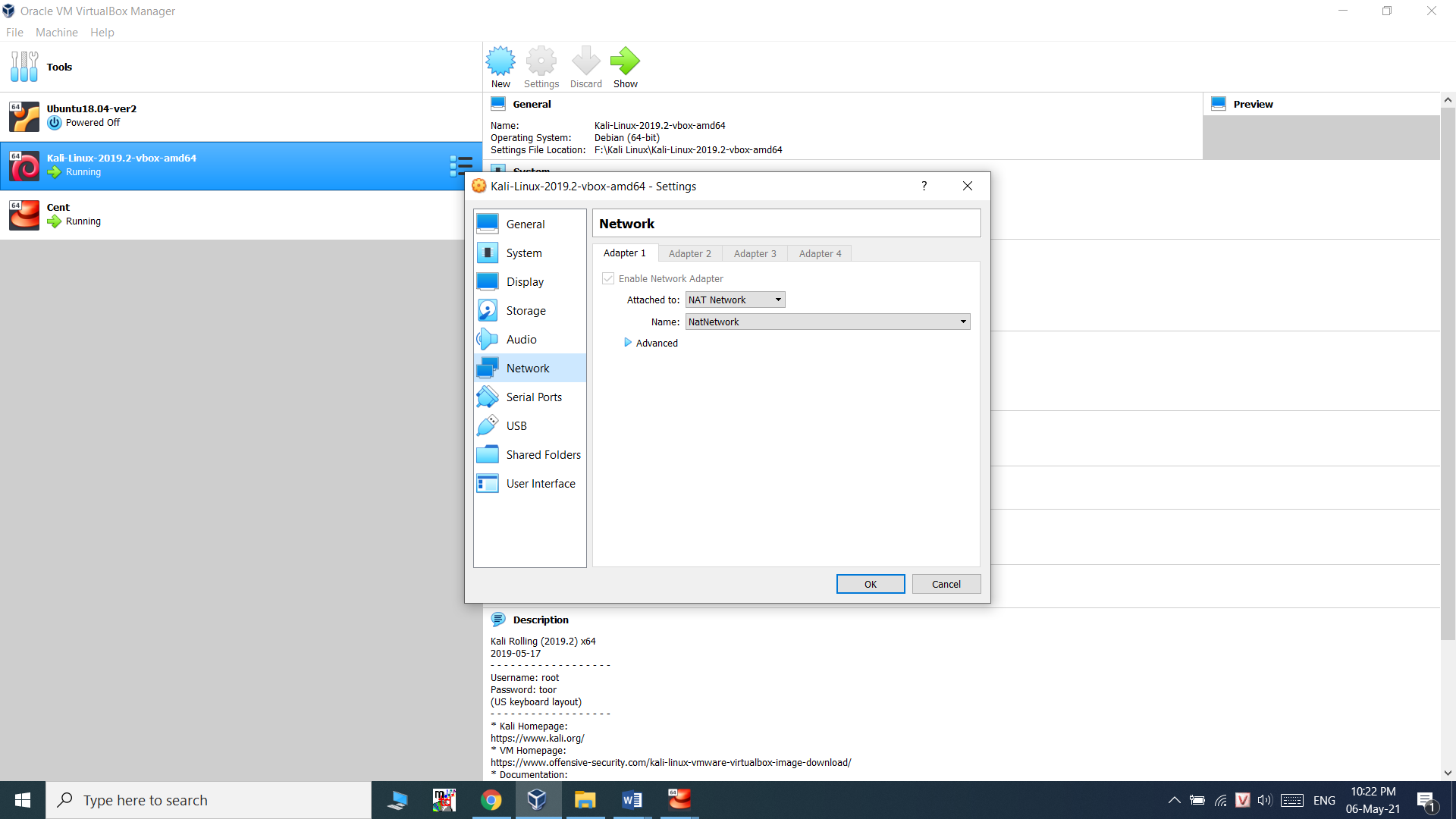
***\* Cấu hình:***

1. Tools -> Preferences -> Network -> Tạo NAT mới

2. Với CentOS và Kali Linux, lần lượt cái đặt NAT network mới vừa được tạo

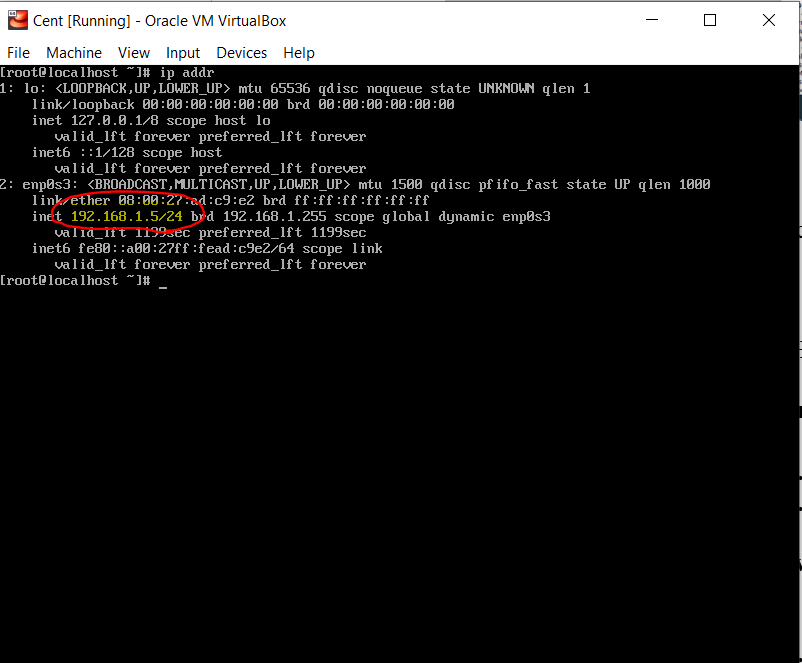




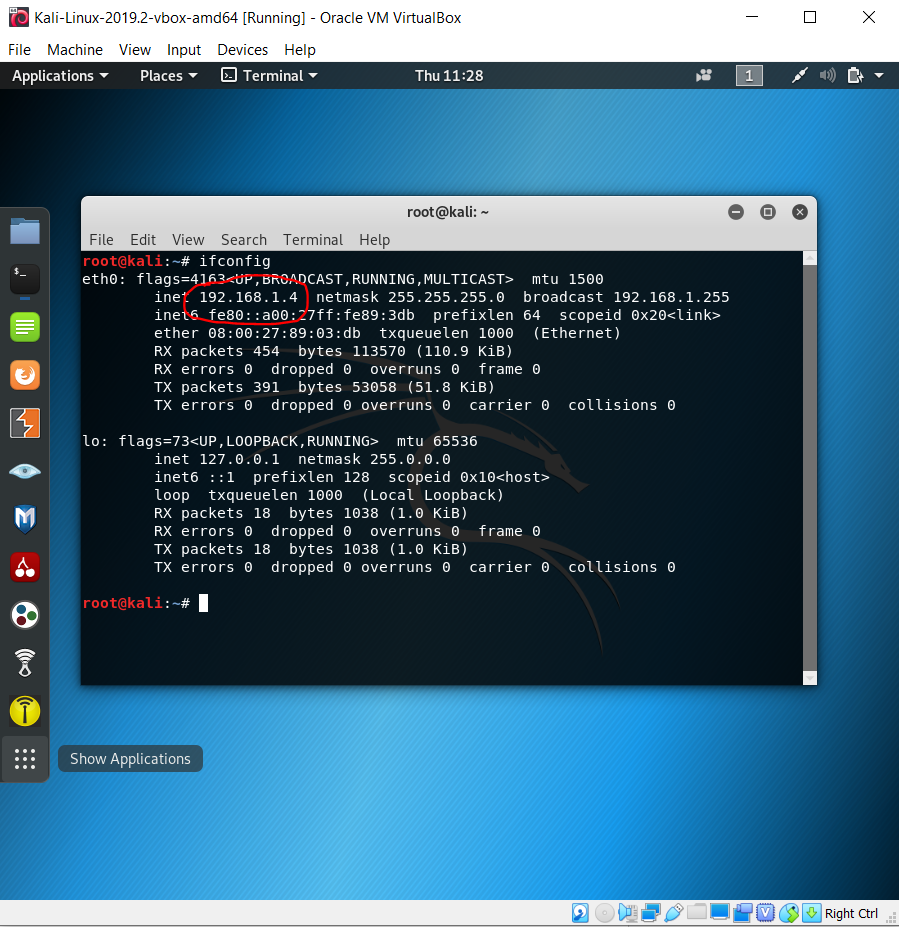


***\* Kết quả lệnh ping:***

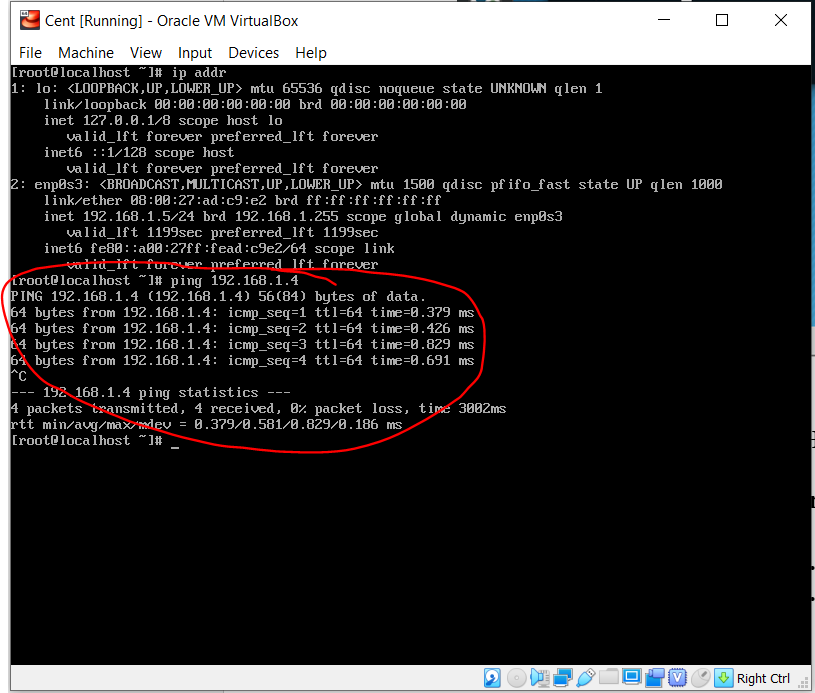
Sau khi đăng nhập CentOS, chạy cmd: **dhclient** sau đó chạy cmd: **ip addr** để xem địa chỉ ip

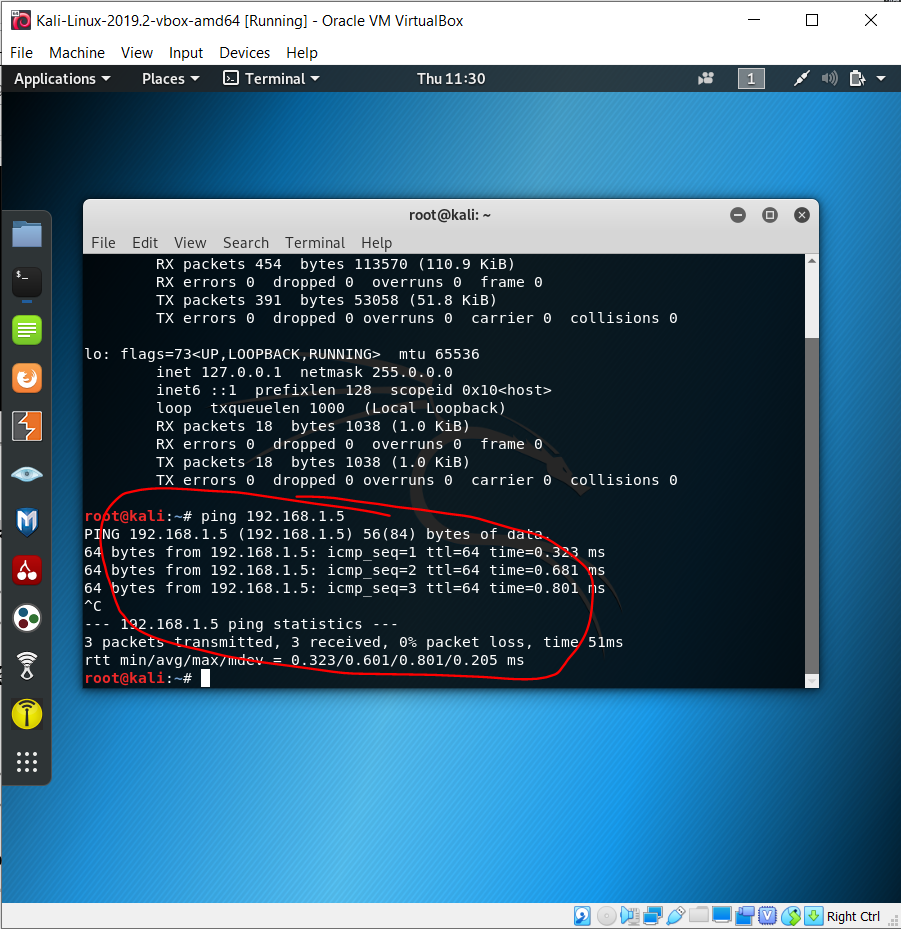


Trên Kali Linux, chạy cmd: **ifconfig** để xem địa chỉ ip



Kết quả ping từ hai phía:





* + - * 1. 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 dùng để tấn công vét cạn username và password thông qua nhiều dịch vụ khác nhau (ssh, ftp, telnet, …). Hydra sẽ lần lượt thử từng username và password cho đến khi đăng nhập thành công vào hệ thống.

Đây là một công cụ đã được cài đặt sẵn trên kali linux.

Cú pháp sử dụng cơ bản:

hydra [-l USERNAME | -L USERNAME\_FILE] [-p PASSWORD | -P PASSWORD\_FILE] [service] [–t TASKS] [–V]

**service** có thể là ssh, ftp, …

**-V** dùng để hiện cặp username/password ở mỗi lần thử.

**TASKS** là số lần kết nối đồng thời.

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

Từ điển **rockyou** đang được nén trong **/usr/share/wordlists** dưới dạng file **rockyou.txt.gz.**

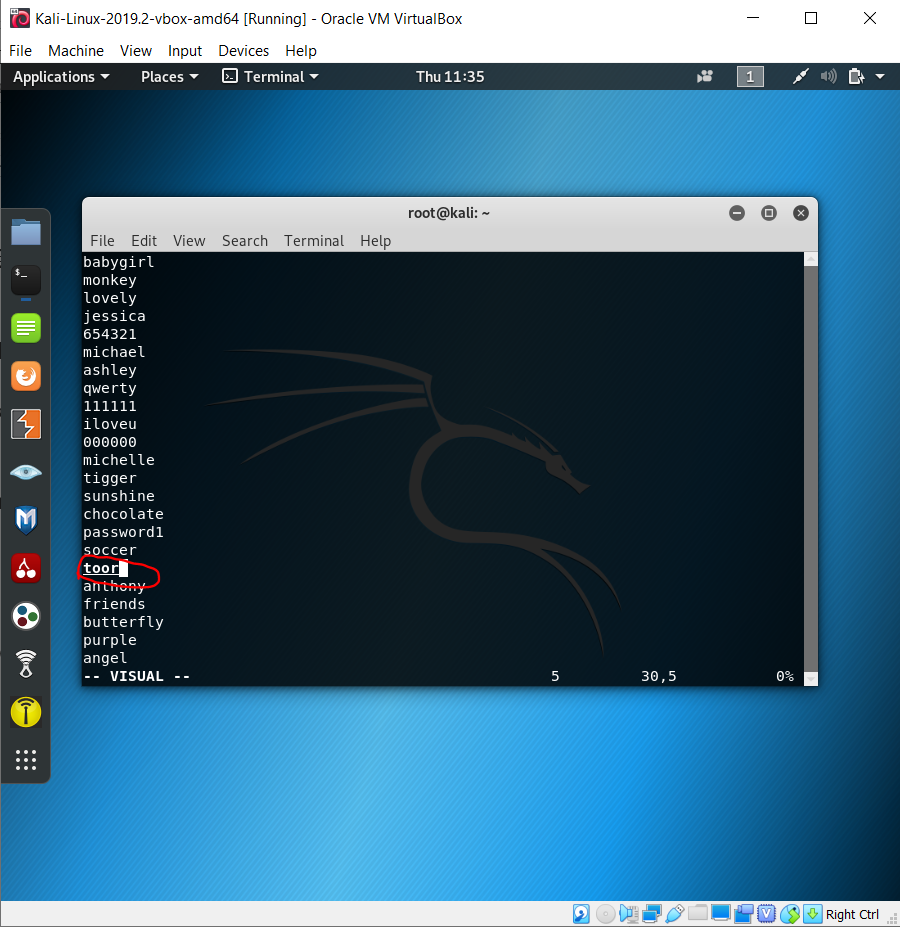
Copy file ra home directory:

***root@kali:~#*** *cp /usr/share/wordlists/rockyou.txt.gz ~*

Giải nén:

***root@kali:~#*** *gunzip rockyou.txt.gz*

Để thuận tiện cho demo, thêm dòng **toor** (mật khẩu của user **root** trên CentOS) vào file **rockyou.txt**.



Khởi động ssh client trên máy kali:

***root@kali:~#*** *service ssh start*

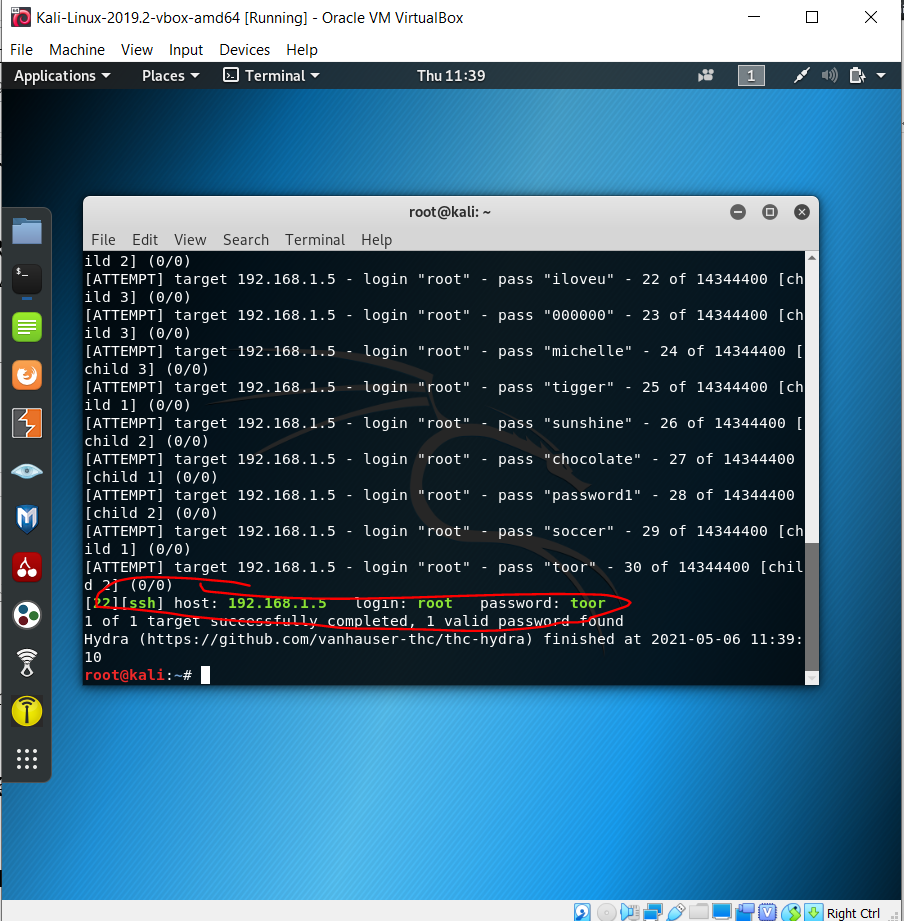
Khởi động ssh daemon trên máy CentOS:

***[root@localhost ~]#*** *service sshd start*

Trên máy kali, bắt đầu sử dụng Hydra:

Dò mật khẩu của user **root**

***root@kali:~#*** *hydra –V –l root –P rockyou.txt 192.168.1.5 ssh –t 4*



* **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:**

***Cú pháp sử dụng crunch:***

*crunch len1 len2 setOfChar –o destination*

*len1*: độ dài tối thiếu của từ

*len2*: độ dài tối đa của từ

*setOfChar*: tập các kí tự để tạo danh sách từ

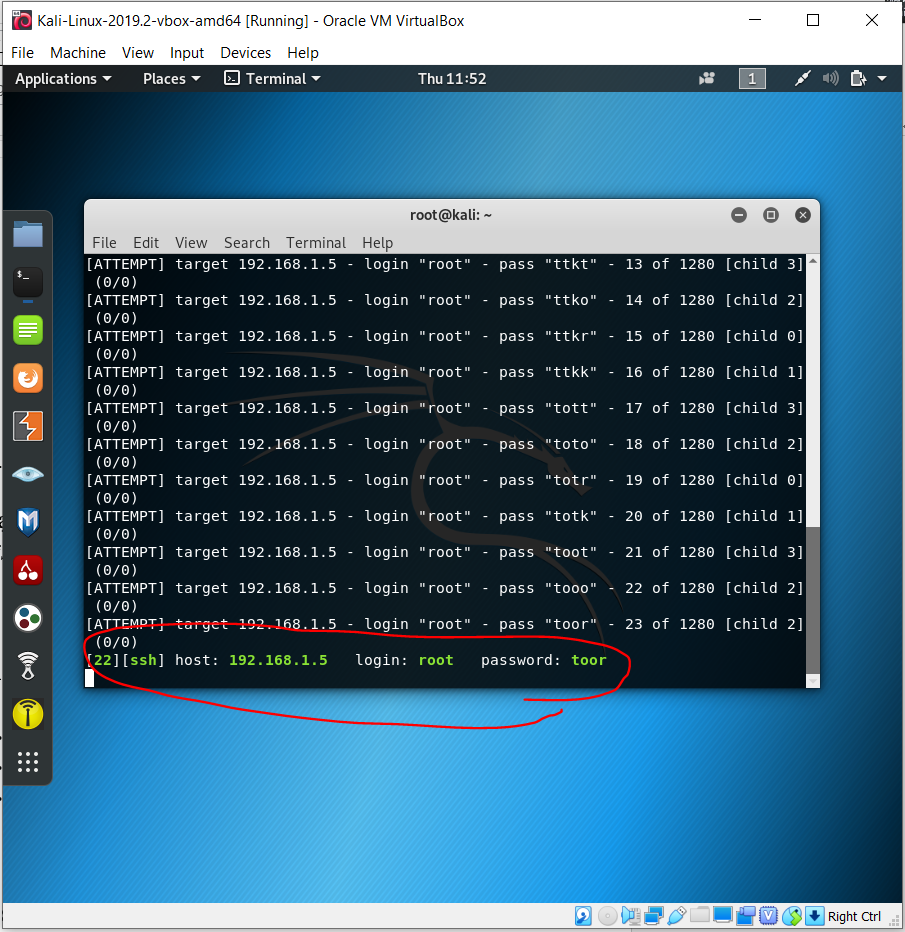
*destination*: file để lưu kết quả

*Ví dụ ta muốn tấn công user* ***root*** *và ta đoán được mật khẩu sẽ có số kí tự từ 4 đến 5 và có thể được tạo nên từ các kí tự* ***t,o,r,k****, ta chạy* ***cmd*** *sau để tạo từ điển:*

***root@kali:~#*** *crunch 4 5 tork -o mywordlist.txt*

Dò mật khẩu của user **root** với từ điển vừa tạo

***root@kali:~#*** *hydra –V –l root –P mywordlist.txt 192.168.1.5 ssh –t 4*



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

Những mật khẩu yếu (ngắn, pattern dễ đoán (tên, ngày sinh, 1234, 0000, …), số ký tự khác nhau không nhiều, dùng các ký tự thường được sử dụng) sẽ dễ dàng bị tấn công bởi hình thức tấn công vét cạn. Những mật khẩu mạnh (dài, không chứa pattern dễ đoán, sử dụng kết hợp chữ, số, các ký tự đặc biệt,…) sẽ tốn rất nhiều thời gian để có thể tìm ra bằng tấn công vét cạn.

* + - * 1. Giải pháp giảm thiểu tấn công vét cạn
* **Tìm hiểu fail2ban và cho biết nó được sử dụng để làm gì ?**

Fail2ban là ứng dụng phân tích log (nhật ký) hệ thống để biết được các dấu hiệu của một cuộc tấn công vào server. Khi xác định được IP bị nghi ngờ là kẻ tấn công, dựa vào các tham số định trước, IP đó sẽ bị đưa vào iptables để block trong một khoảng thời gian hoặc mãi mãi.

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

***Cài đặt:***

***[root@localhost ~]#*** *yum install epel-release*

***[root@localhost ~]#*** *yum install fail2ban*

***Cấu hình:*** *tạo file cấu hình như sau*

***[root@localhost ~]#*** *vi /etc/fail2ban/jail.local*



Trong đó

**enabled**: kích hoạt bảo vệ, nếu muốn tắt chuyển thành false

**filter**: giữ mặc định để sử dụng file cấu hình /etc/fail2ban/filter.d/sshd.conf

**action**: fail2ban sẽ ban địa chỉ IP nếu match filter /etc/fail2ban/action.d/iptables.conf.

**logpath**: đường dẫn file log fail2ban sử dụng để theo dõi

**maxretry**: số lần login false tối đa

**bantime**: thời gian ban IP 3600 giây = 1 giờ

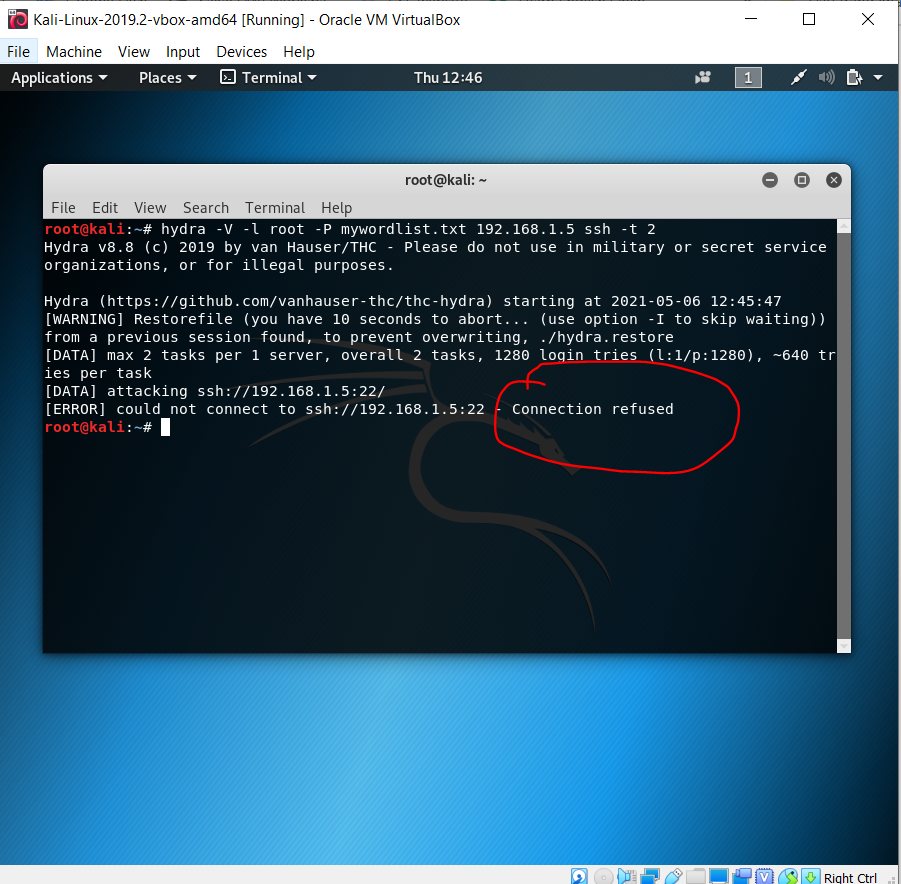
**Khợi động fail2ban:**

***[root@localhost ~]#*** *systemctl enable fail2ban*

***[root@localhost ~]#*** *systemctl start fail2ban*

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

Tấn công thất bại



Xem Ip bị chặn trên CentOS:

***[root@localhost ~]#*** *fail2ban-client status sshd*

