

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA CÔNG NGHỆ THÔNG TIN 1



BÀI THỰC HÀNH 14
THỰC TẬP CƠ SỞ

Họ và tên : Đinh Quang Hiếu

Mã sinh viên: B19DCAT065

Giảng viên giảng dạy: Hoàng Xuân Dậu

HÀ NỘI, THÁNG 5/2022

Bài 14: Phát hiện lỗ hổng với công cụ tìm kiếm

I. Lý thuyết

1.Shodan

Shodan là một công cụ tìm kiếm khác nhiều so với các công cụ tìm kiếm nội dung như Google, Yahoo hoặc Bing. Shodan là một công cụ tìm kiếm để tìm các thiết bị trực tuyến trên internet như: máy tính, server, webcam, các thiết bị routers... Nó hoạt động bằng cách quét toàn bộ các các thiết bị trên internet có mở cổng public ra internet và thực hiện phân tích các dấu hiệu được phản hồi về từ các thiết bị. Sử dụng thông tin đó, Shodan có thể cho bạn biết những thứ như máy chủ web (và phiên bản) nào phổ biến nhất hoặc có bao nhiêu máy chủ FTP ẩn danh tồn tại ở một vị trí cụ thể, hay trả về danh sách các camera có thể truy cập trực tuyến qua internet. Nói chung, với shodan bạn có thể tìm kiếm bất cứ thiết bị nào trên internet miễn là chúng đang có kết nối internet và mở cổng public.

- Shodan (Sentient Hyper-Optimized Data Access Network) hoạt động theo thuật toán sau:

- Tạo một địa chỉ IPv4 (IPV4 là gì) một cách ngẫu nhiên.
- Chọn port (cổng dịch vụ) ngẫu nhiên và thực hiện gửi câu lệnh kiểm tra
- Xem nội dung phản hồi của thiết bị (Service Banner) từ đó xác định xem đó là loại thiết bị gì và chạy cổng gì
- Lặp lại quá trình trên nhưng với ip và port mới. Điều này giúp tạo ra sự ngẫu nhiên cũng như đảm bảo tránh gây ra lượng kết nối quá lớn tới một thiết bị một cách liên tục.

Các cổng dịch vụ mà shodan thường xuyên rà quét: (Port 554 – Real Time Streaming Protocol, Port 5060 – SIP, Port 25 – SMTP, Port 161 – SNMP, Port 23 - Telnet, Port 993 – IMAP, Port 22 – SSH, Port 21 – FTP, Ports 8443, 443, 8080, and 80 – HTTPS/HTTP)

2. Google hacking

Google Hacking là một thuật ngữ mà gói gọn một loạt các kĩ thuật cho phép truy vấn trên công cụ tìm kiếm Google.com, đôi khi được dùng để xác định các lỗ hổng trong các ứng dụng web cụ thể. (Cụ thể như thế nào thì mình sẽ cố gắng giải thích tiếp trong giới hạn kiến thức mà mình biết). Bên cạnh việc truy vấn từ google có thể tiết lộ các lỗ hổng trong các ứng dụng web, Google Hacking cho phép bạn tìm các dữ liệu nhạy cảm, có ích cho giai đoạn Reconnaissance để attack ứng dụng, chẳng hạn như email liên kết với một trang web nào đó, cơ sở dữ liệu hoặc các file khác với tên người dùng và mật khẩu, các thư mục không được bảo vệ với các tập tin nhạy cảm, URL để đăng nhập cổng thông tin, các loại khác nhau của các bản ghi hệ thống như tường lửa và truy cập các bản ghi....

- Google hacking database chia thành nhiều loại khác nhau như: thông tin các file bị tổn thương, các file chứa mật khẩu, thông tin về máy chủ và phần mềm trên đó, tìm kiếm các thiết bị trực tuyến...etc. Một Dork chỉ là một truy vấn Google đã tìm ra kết quả hữu ích như khai thác dữ liệu nhạy cảm. Khi duyệt qua các kết quả, bạn nên tham khảo đến thời gian update hoặc thời gian được lưu trữ, Google hỗ trợ điều đó rất tốt từ các kết quả mà nó mang lại cho bạn. Một vài kết quả từ lâu sẽ bao gồm là các thông tin phiên bản ứng dụng gặp lỗi, lỗi ứng dụng code,...

- Hiện tại chúng tôi ngày càng có nhiều IOT Thiết bị (Internet of Things), tự động hóa gia đình và nhiều hơn nữa được kết nối với Internet. Vấn đề mà họ gặp phải là chúng bị xử lý bởi những người không có đủ kiến thức hoặc thiết bị này không được trang bị các biện pháp bảo mật cần thiết. Sau đó, chúng tôi tìm thấy các lỗi như mật khẩu mặc định, cấu hình xấu và thiết bị do thiếu bản cập nhật nên ngày càng trở nên không an toàn.

Một số ví dụ có thể bị ảnh hưởng là camera giám sát video, TV thông minh, máy in, v.v. Ví dụ, đối với camera giám sát video, chúng tôi có thể sử dụng:

- máy ảnh linksys inurl: main.cgi
- intitle: "camera mạng toshiba - Đăng nhập người dùng"

Thay vào đó, đối với máy in:

- inurl: webarch / mainframe.cgi
- intitle: "network print server" filetype: shtml
- Các chức năng Hacking khác của Google mà chúng tôi có thể thực hiện thông qua việc sử dụng các toán tử sẽ là:
 - Tìm kiếm các máy chủ lỗi thời và dễ bị tấn công.
 - Thực hiện tìm kiếm người dùng và mật khẩu của các trang web, máy chủ và cơ sở dữ liệu.

Để kết thúc với Google Hacking, cần lưu ý rằng thông tin này có sẵn do cấu hình máy chủ hoặc thiết bị không tốt, thiếu các bản cập nhật và cũng vì Google đôi khi lập chỉ mục những thông tin không nên

II. Thực Hành

1. Thử nghiệm với Shodan

- tìm máy chủ apache và có hostname .ptit.edu.vn

TOTAL RESULTS

4

View Report

View on Map

New Service: Keep track of what you have connected to the

jobs.ptit.edu.vn – Trang web thông tin việc làm sinh viên Học viện

203.162.88.104

static.vnpt.vn

ptit.edu.vn

Centre for development of

information technology

Viet Nam, Hanoi

php

SSL Certificate

Issued By:

Common Name:

AlphaSSL CA - SHA256 -

G2

Organization:

GlobalSign nv-sa

Issued To:

Common Name:

*.ptit.edu.vn

Supported SSL Versions:

TLSv1, TLSv1.1, TLSv1.2,

TLSv1.3

Diffie-Hellman Fingerprint:

RFC3526/Oakley Group 14

HTTP/1.1 200 OK

Date: Sun, 15 May 2022 16:27:37 GMT

Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.3.9

X-Powered-By: PHP/7.3.9

Set-Cookie: PHPSESSID=hk6kp9b0f086crv0qutmbjsmp; path=

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-c...

Viện công nghệ Thông tin và Truyền thông CDIT

203.162.10.106

static.vnpt.vn

SSL Certificate

Issued By:

HTTP/1.1 301 Moved Permanently

Date: Fri, 13 May 2022 04:08:31 GMT



TRANG CHỦ

GIỚI THIỆU

HỒ SƠ

VIỆC LÀM

VIỆC LÀM MỚI

ĐĂNG NHẬP

Việc làm theo nhóm ngành nghề



IT-Hệ thống

(1 việc làm)



Kế toán

(1 việc làm)



Kinh doanh

(1 việc làm)



Lập trình

(1 việc làm)



Thiết kế

(0 việc làm)



Truyền thông

(0 việc làm)

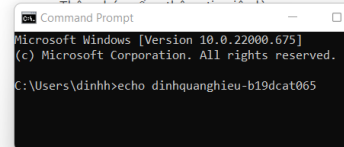
Xem thêm

Thông báo



Thông báo cổng
thông tin việc làm
bắt đầu hoạt động từ
1/10

Share



Đọc tiếp

- tìm máy chủ web IIS ở hà nội

apsImagesMonitorDeveloperMore...

ANExploreDownloadsPricing ↗web iis city:HaNoi

.TS

View ReportView on Map

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

14.248.82.141 ↗

Vietnam Posts and Telecommunications Group

Viet Nam, Hanoi

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/7.5
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Thu, 19 May 2022 00:41:34 GMT
Content-Length: 2897

<!DOCTYPE html>
<html>
<head>
 <meta charset=...

33

9

7

7

6

ZATIONS

ists and Telecommunications

up

om Infrastructure Company

m

c Network Information Centre

43

17

7

6

4

112.72.98.69 ↗

VTC Wireless Broadband Company

Viet Nam, Hanoi

HTTP/1.1 401 Unauthorized
Content-Length: 1539
Content-Type: text/html
Server: Microsoft-IIS/6.0
WWW-Authenticate: Negotiate
WWW-Authenticate: NTLM
X-Powered-By: ASP.NET

```
Microsoft Windows [Version 10.0.22000.675]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\dinh>echo dinhquanghieu-b19dcat065
```

shodan.io/host/14.248.82.141

14.248.82.141

Regular ViewRaw DataHistory

General Information

Country

Viet Nam

City

Hanoi

Organization

Vietnam Posts and Telecommunications Group

ISP

VNPT Corp

ASN

AS45899

Web Technologies

ROOTSTRAB

LOJIEV

MOJENI7D

Command Prompt

```
Microsoft Windows [Version 10.0.22000.675]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\dinh>echo dinhquanghieu-b19dcat065
```

11131517192

43495370798

919810210411011

17919522122226431

46550351554855458

87390299299399510

1177120013111344135513

- tìm những thiết bị mở port 22 tại việt nam

SHODAN

Explore

Downloads

Pricing

port:22 country:vn

TOTAL RESULTS

84,133

TOP CITIES

Hanoi

32,391

Ho Chi Minh City

29,377

Da Nang

1,583

Biên Hòa

1,009

Haiphong

761

More...

TOP ORGANIZATIONS

Vietnam Posts and Telecommunications Group

15,900

Viettel Group

11,001

FPT Telecom Company

3,469

FPT Telecom

2,225

View Report

Browse Images

View on Map

New Service: Keep track of what you have connected to the Internet. [CHC:Users\dinghh>echo dinghuanghieu-b19dcat065](#)

103.148.57.124

Viva social network Joint Stock Company

Viet Nam, Hanoi

SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3

Key type: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAADAQABAAQDHzi1whvoya0Z+oeDEcBZspshdn4tprxxS7ZqvF8I2+qCn

hwG3ac9PHozjN6b1S13rPXn33uoa/OeDmN21LYsfeGz2gVXLZeedBUXu6/U4a1wk+EhshVPEMK6E

0cT3ktig1b4FsD764brr8Dyxtti2F6+xdck1Jhzb1pf4Jq75VKyFosKXxryppQDvb7eJX2EsZcR

00j...

103.238.81.16

Cloudone Technology Company Limited

Viet Nam, Hanoi

SSH-2.0-OpenSSH_5.3

Key type: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAABIAAAQEAvgVhV01CpLxbVC10aF8JKt7gU76bujsualNDHFUx0+Tm48nk

bDehVsvp+qUBRoTEh18uwmFH0z3ZtpeI83a0Gd+LA26sVYpHw/AaC0xcjWKF+ZfVzP4u7Jw7Cr

/57Q/b/r0HlIjNruW44bpVKlW7tyUvD05qfCKHh5ZuZ2VvkZvUF3M/TeZ0xcgLoF6sjapv1ssZ

ynuHnIbrcv8/VB50C1IKVml...

45.125.236.183

shodan.io/host/103.148.57.124

Shodan

Maps

Images

Monitor

Developer

More...

SHODAN

Explore

Downloads

Pricing

Search...

103.148.57.124

Regular View

Raw Data

History

General Information

Country

Viet Nam

City

Hanoi

Organization

Viva social network Joint Stock Company

ISP

VNPT Corp

ASN

AS45899

Operating System

Ubuntu

Open Ports

22

1883

8080

// 22 / TCP

OpenSSH 7.6p1 Ubuntu-4ubuntu0.3

SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3

Key type: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAADAQABAAQDHzi1whvoya0Z+oeDEcBZspshdn4tprxxS7ZqvF8I2+qCn

hwG3ac9PHozjN6b1S13rPXn33uoa/OeDmN21LYsfeGz2gVXLZeedBUXu6/U4a1wk+EhshVPEMK6E

0cT3ktig1b4FsD764brr8Dyxtti2F6+xdck1Jhzb1pf4Jq75VKyFosKXxryppQDvb7eJX2EsZcR

00j81D4PkH8AUJgd0ab1001wCuaDRB1bpFzAsaPCndsaCu2ciPos4E18zavPhxmpIYR5MuuxFKb

TKESH+0npNAe04U3g75YK6vK1J1RVo6/uXv5o4xIV+3MjNthoRU1w18P1Qs0Yvvg+1dn

Fingerprint: f6:75:ca:85:e6:5d:5b:6c:51:67:8e:5e:25:d3:47:f7

- tìm máy chủ có hostname là .ptit.edu.vn

web technologies

ANIMATE.CSS BOOTSTRAP FONT AWESOME JQUERY

MODERNIZR OWL CAROUSEL SWIPER SLIDER

YOUTUBE

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2018-15919 Remotely observable behaviour in auth-gss2c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or 'oracle') as a vulnerability'.

CVE-2017-15906 The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

Server Host Key Algorithms

- ssh-rsa
- rsa-sha2-512
- rsa-sha2-256
- ecdsa-sha2-NISTP256
- ssh-ed25519

Encryption Algorithms

- chacha20-poly1305
- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes128-gcm@openssh.com
- aes256-gcm@openssh.com
- aes128-cbc
- aes192-cbc
- aes256-cbc
- blowfish-cbc
- cast128-cbc
- 3des-cbc

MAC Algorithms:

- umac-64-etm@openssh.com
- umac-128-etm@openssh.com
- hmac-sha2-256-etm@openssh.com
- hmac-sha2-512-etm@openssh.com
- hmac-sha1-etm@openssh.com
- umac-64@openssh.com
- umac-128@openssh.com
- hmac-sha2-256

- tìm những thiết bị chạy win 7 tại VN

Shodan Maps Images Monitor Developer More...

SHODAN Explore Downloads Pricing

os:windows 7 country:vn

TOTAL RESULTS

923

TOP CITIES

City	Count
Ho Chi Minh City	351
Hanoi	301
Biên Hòa	17
Chi Linh	14
Da Nang	11

More...

TOP PORTS

Port	Count
3389	690
445	230
3388	3

View Report Browse Images View on Map

New Service: Keep track of what you have connected to the Internet. C

103.90.224.117

Vietnix cloud company limited

Viet Nam, Ho Chi Minh City

self-signed

SSL Certificate

Issued By: WIN-FKGTUG3HTEL

Issued To: WIN-FKGTUG3HTEL

Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Fingerprint: RFC2409/Oakley Group 2

Remote Desktop Protocol NTLM Info:

OS: Windows 7/Windows Server 2008 R2

OS Build: 6.1.7601

Target Name: WIN-FKGTUG3HTEL

NetBIOS Domain Name: WIN-FKGTUG3HTEL

NetBIOS Computer Name: WIN-FKGTUG3HTEL

DNS Domain Name: WIN-FKGTUG3HTEL

FQDN: WIN-FKGTUG3HTEL

Administrator

Logged on

kk)

(A

...

- Dùng metasploit để quét webcamxp


```
msf6 > search shodan
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/http/influxdb_enum		normal	No	InfluxDB Enum Utility
1	auxiliary/gather/shodan_honeyscore		normal	No	Shodan Honeyscore Client
2	auxiliary/gather/shodan_host		normal	No	Shodan Host Port
3	auxiliary/gather/shodan_search		normal	No	Shodan Search
4	auxiliary/scanner/http/smt_ipmi_49152_exposure	2014-06-19	normal	No	Supermicro Onboard IPMI Port 49152 Sensitive File Exposure

Interact with a module by name or index. For example `info 4`, use `4` or use `auxiliary/scanner/http/smt_ipmi_49152_exposure`

```
msf6 > use 3
```

```
msf6 auxiliary(gather/shodan_search) > show options
```

Module options (auxiliary/gather/shodan_search):

Name	Current Setting	Required	Description
DATABASE	false	no	Add search results to the database
MAXPAGE	1	yes	Max amount of pages to collect
OUTFILE		no	A filename to store the list of IPs
QUERY		yes	Keywords you want to search for
REGEX	.*	yes	Regex search for a specific IP/City/Country/Hostname
SHODAN_APIKEY		yes	The SHODAN API key

```
msf6 auxiliary(gather/shodan_search) >
```

```
dinhquanghieu-b19dcat065@B19DCAT065-Hieu-Kali: ~  
File Actions Edit View Help  
(dinhquanghieu-b19dcat065@B19DCAT065-Hieu-Kali)-[~]  
$
```

```
msf6 auxiliary(gather/shodan_search) > set shodan_apikey gyXxo2YozqGSZUzgrJ0v1PdfavIQCzF
```

```
shodan_apikey => gyXxo2YozqGSZUzgrJ0v1PdfavIQCzF
```

```
msf6 auxiliary(gather/shodan_search) > set query webcamxp
```

```
query => webcamxp
```

```
msf6 auxiliary(gather/shodan_search) > run
```

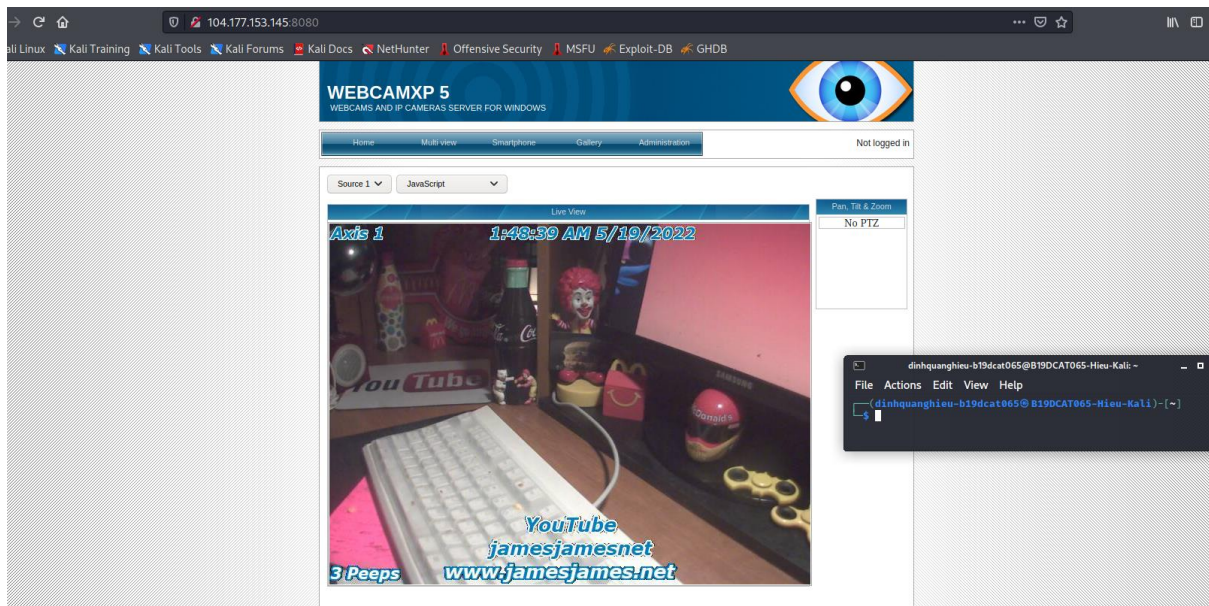
```
[*] Total: 530 on 6 pages. Showing: 1 page(s)
```

```
[*] Collecting data, please wait ...
```

Search Results

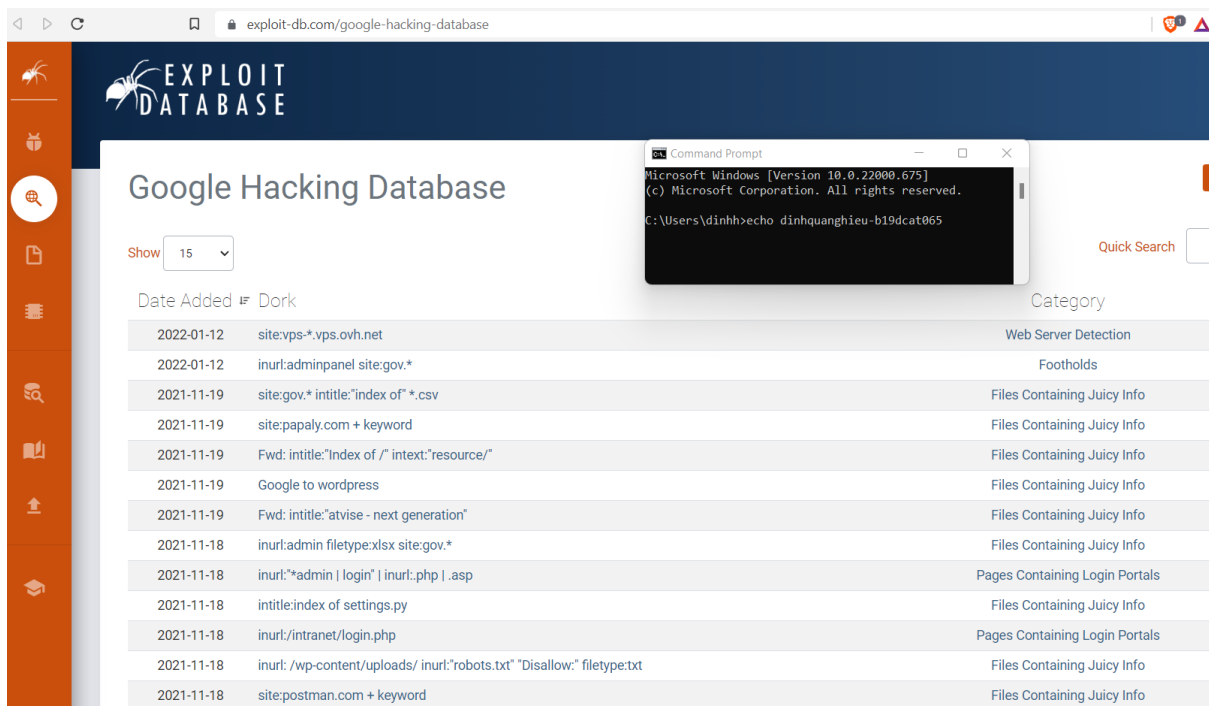
IP:Port	City	Country	Hostname
104.177.153.145:8080	Jacksonville	United States	104-177-153-145.lightspeed.jcvlfl.sb cglobal.net
113.11.181.88:8181	Mojokerto	Indonesia	
130.51.31.219:8080	Idaho Falls	United States	
139.162.119.9:49152	Tokyo	Japan	li1603-9.members.linode.com
139.162.119.9:52869	Tokyo	Japan	li1603-9.members.linode.com
139.162.119.9:80	Tokyo	Japan	li1603-9.members.linode.com
139.162.75.108:4840	Tokyo	Japan	li1555-108.members.linode.com
139.59.122.225:80	Singapore	Singapore	
139.59.56.96:37215	Doddaballapura	India	
139.59.56.96:9000	Doddaballapura	India	
139.64.168.120:8080	Logan	United States	
142.93.221.114:80	Bengaluru	India	
157.245.60.237:80	Singapore	Singapore	
164.92.188.97:80	Frankfurt am Main	Germany	
165.22.109.75:80	Singapore	Singapore	
172.104.143.118:37215	Frankfurt am Main	Germany	li1659-118.members.linode.com
172.104.143.118:49152	Frankfurt am Main	Germany	li1659-118.members.linode.com
172.104.143.118:60001	Frankfurt am Main	Germany	li1659-118.members.linode.com
172.104.143.118:80	Frankfurt am Main	Germany	li1659-118.members.linode.com
172.104.143.118:81	Frankfurt am Main	Germany	li1659-118.members.linode.com

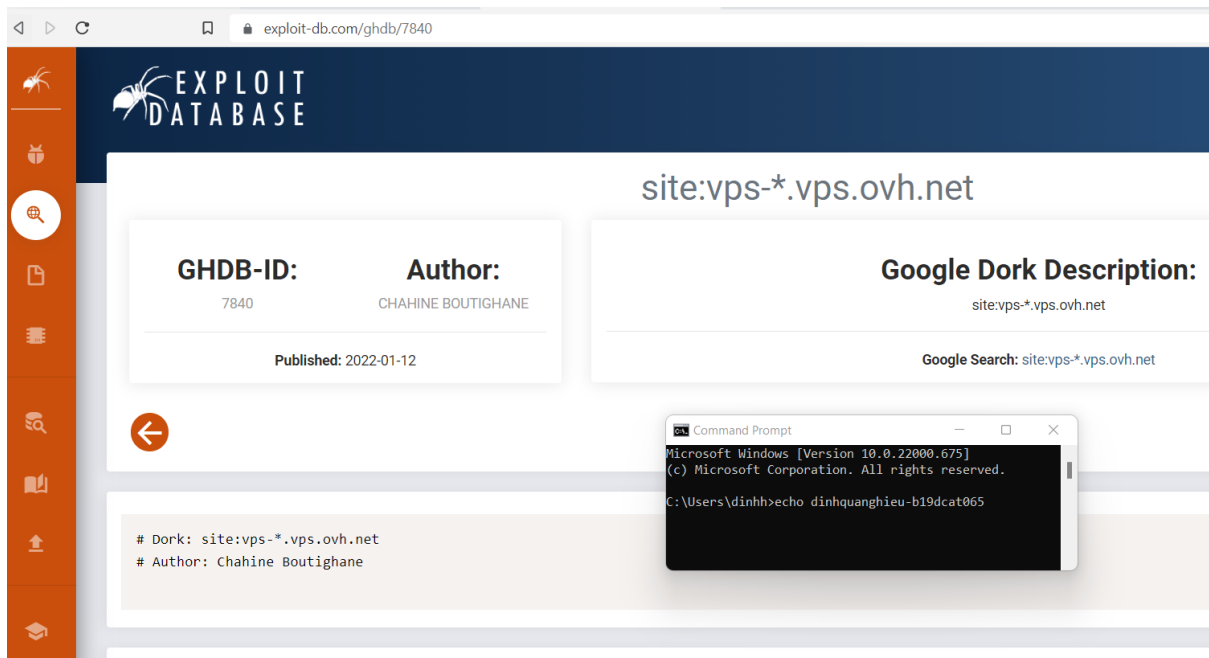
```
dinhquanghieu-b19dcat065@B19DCAT065-Hieu-Kali: ~  
File Actions Edit View Help  
(dinhquanghieu-b19dcat065@B19DCAT065-Hieu-Kali)-[~]  
$
```



2. Thử nghiệm với Google Hacking

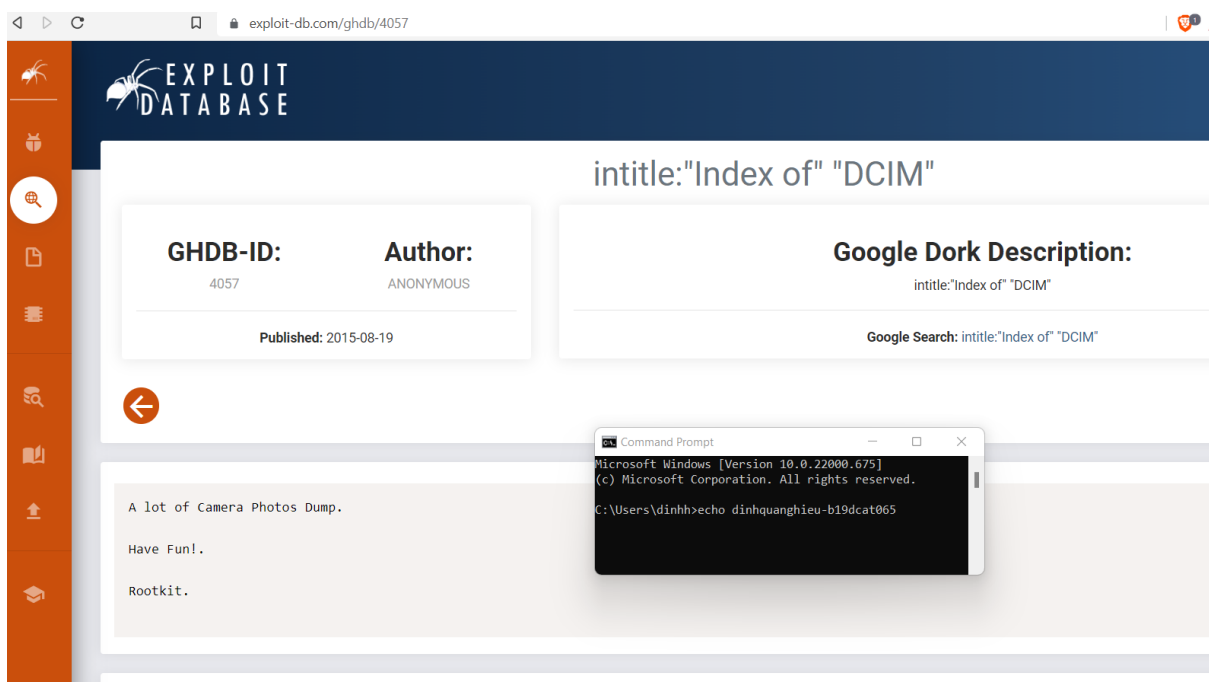
- Filter theo Vulnerable Servers





The screenshot shows the Exploit-DB interface for entry 7840. The search query is `site:vps-*.vps.ovh.net`. The entry details include GHDB-ID: 7840, Author: CHAHINE BOUTIGHANE, and Published: 2022-01-12. The Google Dork Description is `site:vps-*.vps.ovh.net`. A Google Search link is provided: `site:vps-*.vps.ovh.net`. A back arrow icon is visible. A Command Prompt window is overlaid, showing the command `C:\Users\dinh>echo dinhquanghieu-b19dcat065`.

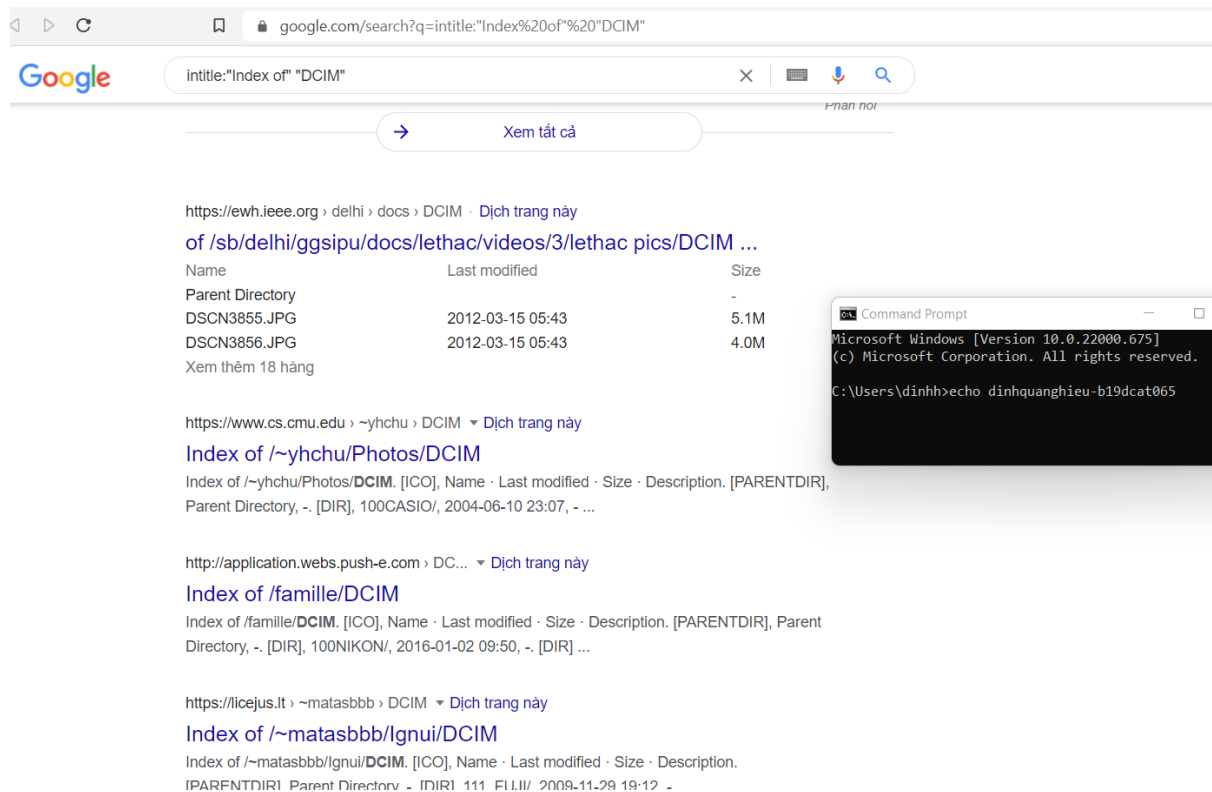
- Chọn một mục để hiện ra trang thông tin có liên quan bao gồm thông tin tác giả, mô tả về tìm kiếm và các thông tin khác.



The screenshot shows the Exploit-DB interface for entry 4057. The search query is `intitle:"Index of" "DCIM"`. The entry details include GHDB-ID: 4057, Author: ANONYMOUS, and Published: 2015-08-19. The Google Dork Description is `intitle:"Index of" "DCIM"`. A Google Search link is provided: `intitle:"Index of" "DCIM"`. A back arrow icon is visible. A Command Prompt window is overlaid, showing the command `C:\Users\dinh>echo dinhquanghieu-b19dcat065`.

- Thử nghiệm với ví dụ: `www.exploit-db.com/ghdb/4057`. Với truy vấn tìm kiếm `intitle:"Index of" "DCIM"`, Google sẽ trả về kết quả của các bộ sưu tập ảnh mà mọi người không biết ở đó. Sinh viên cần tìm hiểu các từ khóa trong câu lệnh: `intitle`, `DCIM`.

- intitle: giúp Google giới hạn kết quả tìm kiếm về những trang có chứa từ đó trong tiêu đề. VD: intitle: "Index of" "DCIM" sẽ trả về những trang có từ "Index of", "DCIM" trong tiêu đề
- Mục DCIM thực chất là từ viết tắt của Digital Camera Images. Đó là tên thư mục trong Quy tắc thiết kế cho hệ thống Tập máy ảnh, là một phần của hệ thống tập máy ảnh kỹ thuật số




























The screenshot shows a Google search result for the query "intitle:Index of \"DCIM\"". The search results list several directories, including one from <https://ewh.ieee.org> and another from <https://www.cs.cmu.edu>. The first result shows a directory listing for <https://ewh.ieee.org/delhi/docs/DCIM> with a table of files:

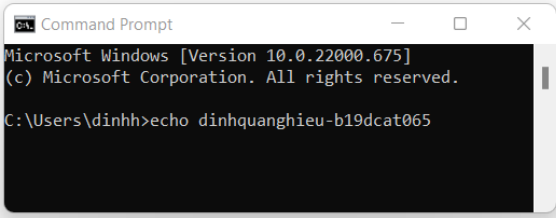
Name	Last modified	Size
Parent Directory	-	-
DSCN3855.JPG	2012-03-15 05:43	5.1M
DSCN3856.JPG	2012-03-15 05:43	4.0M

Below the table, it says "Xem thêm 18 hàng". To the right of the search results, a Windows Command Prompt window is open, showing the command `C:\Users\đinh>echo đínghuỳnhieu-b19dcat065` and its output.

licejus.lt/~matasbbb/Ignui/DCIM/111_FUJI/

Index of /~matasbbb/Ignui/DCIM/111_FUJI

Name	Last modified	Size	Description
 Parent Directory	-	-	-
 DSCF1013.JPG	2009-11-28 23:55	4.8M	
 DSCF1014.JPG	2009-11-28 23:56	4.8M	
 DSCF1015.JPG	2009-11-28 23:57	4.7M	
 DSCF1016.JPG	2009-11-28 23:57	4.7M	
 DSCF1017.JPG	2009-11-29 19:05	4.5M	
 DSCF1019.JPG	2009-11-29 19:05	4.6M	
 DSCF1022.JPG	2009-11-29 19:05	4.5M	
 DSCF1023.JPG	2009-11-29 00:01	4.5M	
 DSCF1024.JPG	2009-11-29 00:01	4.7M	
 DSCF1025.JPG	2009-11-29 00:02	4.0M	
 DSCF1026.JPG	2009-11-29 19:05	4.3M	
 DSCF1027.JPG	2009-11-29 19:05	4.6M	
 DSCF1028.JPG	2009-11-29 19:05	4.4M	
 DSCF1029.JPG	2009-11-29 19:05	4.5M	
 DSCF1030.JPG	2009-11-29 19:05	4.4M	
 DSCF1032.JPG	2009-11-29 19:05	4.7M	
 DSCF1034.JPG	2009-11-29 01:06	4.6M	
 DSCF1037.JPG	2009-11-29 01:10	4.7M	
 DSCF1038.JPG	2009-11-29 01:10	4.7M	
 DSCF1039.JPG	2009-11-29 01:10	4.7M	
 DSCF1040.JPG	2009-11-29 01:10	4.7M	
 DSCF1041.JPG	2009-11-29 01:10	4.8M	
 DSCF1042.JPG	2009-11-29 01:10	4.7M	
 DSCF1044.JPG	2009-11-29 01:11	4.2M	



```
Microsoft Windows [Version 10.0.22000.675]
(c) Microsoft Corporation. All rights reserved.

C:\Users\dinh>echo dinhquanghieu-b19dcat065

dinhquanghieu-b19dcat065
```

- Tìm hiểu lệnh (còn gọi là Google dork) tại www.exploitdb.com/ghdb/6322 để tìm các khóa SSH.

exploit-db.com/ghdb/6322

EXPLOIT DATABASE

intitle:"index of" "id_rsa.pub"

GHDB-ID:
6322

Author:
SID JOSHI

Published: 2020-06-22

Google Dork Description:
intitle:"index of" "id_rsa.pub"

Google Search: intitle:"index of" "id_rsa.pub"

```
# Dork: intitle:"index of" "id_rsa.pub"
# Author: Sid Joshi
# Result of this dorks contains Sensitive Directories with juicy ssh keys.

# POC in attachment

# Thanks!
```

```
Microsoft Windows [Version 10.0.22000.675]
(c) Microsoft Corporation. All rights reserved.

C:\Users\dinh>echo dinhquanghieu-b19dcat065
```

Not secure | 164.177.30.131/apiAgro/puphpet/files/dot/ssh/

Index of /apiAgro/puphpet/files/dot/ssh

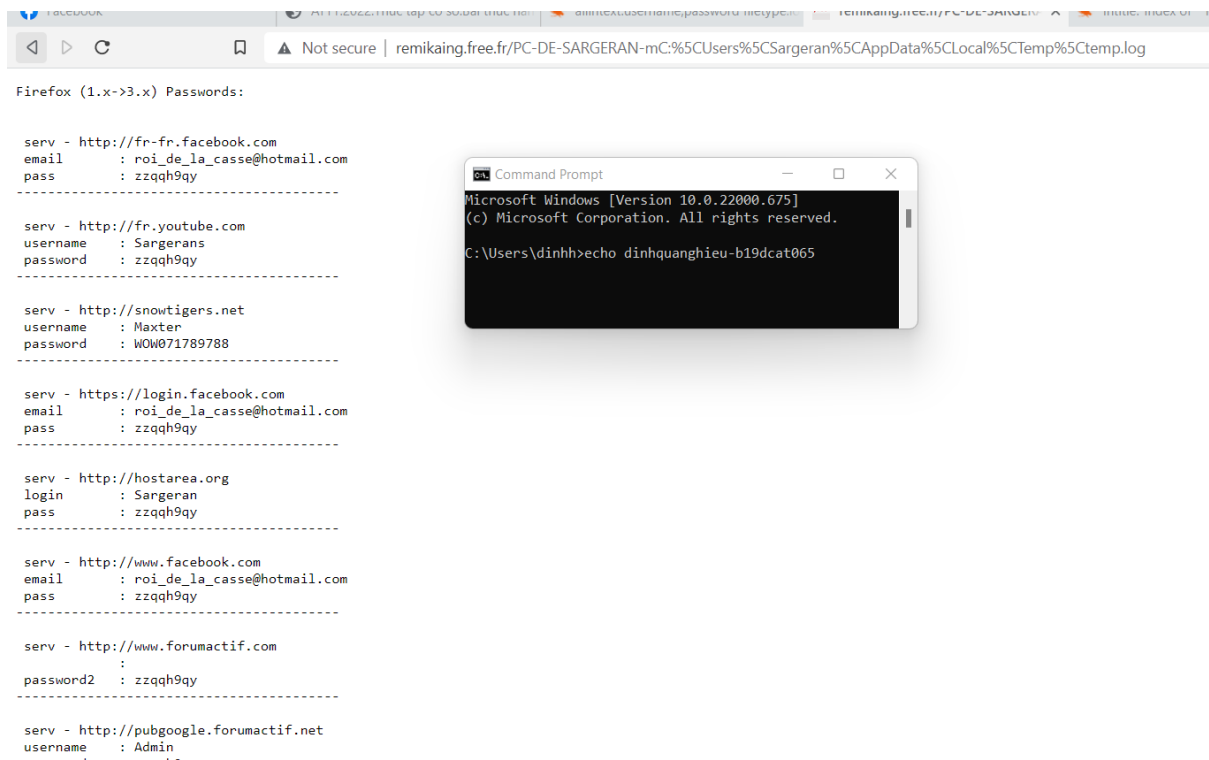
Name	Last modified	Size	Description
Parent Directory	-	-	-
id_rsa	2015-11-02 17:20	1.6K	
id_rsa.ppk	2015-11-02 17:20	1.4K	
id_rsa.pub	2015-11-02 17:20	392	
insecure_private_key	2015-11-02 17:20	1.6K	
root_id_rsa	2015-11-02 17:20	1.6K	
root_id_rsa.ppk	2015-11-02 17:20	1.4K	
root_id_rsa.pub	2015-11-02 17:20	392	

Apache/2.4.10 (Debian) Server at 164.177.30.131 Port 80

```
Microsoft Windows [Version 10.0.22000.675]
(c) Microsoft Corporation. All rights reserved.

C:\Users\dinh>echo dinhquanghieu-b19dcat065
```

- Tìm hiểu Google dork tại www.exploit-db.com/ghdb/6412 tìm log có tên người dùng và mật khẩu, có thể có các mục khác như địa chỉ e-mail, URL mà những thông tin đăng nhập này được sử dụng, v.v



- Thư mục gốc của máy chủ ftp.riken.jp



Browser address bar: <https://ftp.axoft.com/ftp/>

Index of /ftp

Name	Last modified	Size	Description
Parent Directory		-	
Epson/	2019-05-30 10:00	-	
FEX/	2017-01-11 17:13	-	
docs/	2017-01-11 17:13	-	
info/	2022-05-11 10:24	-	
iso/	2020-04-13 09:20	-	
manuales/	2018-11-20 16:30	-	
net461/	2018-04-25 13:12	-	
prjIncidentesClient.exe	2011-11-16 18:58	5.7M	
pub/	2018-08-07 15:15	-	
remoto/	2018-04-18 13:15	-	
seminarios/	2018-10-30 18:10	-	
soporteretail/	2017-01-11 17:13	-	
sqlxpress/	2017-01-11 17:13	-	
tango/	2021-02-26 18:25	-	
tango_educativa/	2018-02-27 16:57	-	
tango.net/	2019-01-18 10:20	-	
tecnica/	2022-04-30 12:00	-	
temp/	2017-11-15 11:32	-	
tupdate/	2019-09-24 15:00	-	
version_interna/	2022-03-21 09:42	-	
vpn/	2021-08-11 13:38	-	

Command Prompt

```
Microsoft Windows [Version 10.0.22000.675]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\dinh>echo dinhquanghieu-b19dcat065
```

- Xem các file log của máy chủ ftp

Browser address bar: exploit-db.com/ghdb/5716

EXPLOIT DATABASE

intitle:"index of" "ftp.log"

GHDB-ID: 5716

Author: PANKAJ KUMAR THAKUR

Published: 2020-01-28

Google Dork Description:

intitle:"index of" "ftp.log"

Google Search: intitle:"index of" "ftp.log"

←

Dork: intitle:"index of" "ftp.log"

Author: Pankaj Kumar Thakur (Nepal)
Linkedin: <https://www.linkedin.com/in/pankaj1261/>
Twitter: @Nep_1337_1998

Info:
It contains FTP LOGS

Command Prompt

```
Microsoft Windows [Version 10.0.22000.675]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\dinh>echo dinhquanghieu-b19dcat065
```


Index of /logs

Name	Last modified	Size	Description
Parent Directory	-		
access.log.36.gz	2011-05-31 09:57	42K	
access.log.37.gz	2011-05-31 09:57	43K	
access.log.38.gz	2011-05-31 09:57	82K	
access.log.39.gz	2011-05-31 09:57	86K	
access.log.40.gz	2011-05-31 09:58	101K	
access.log.41.gz	2011-05-31 09:58	86K	
access.log.42.gz	2011-05-31 09:58	103K	
access.log.43.gz	2011-05-31 09:58	208K	
access.log.44.1.gz	2011-05-31 09:58	65K	
access.log.44.2.gz	2011-05-31 09:58	51K	
access.log.44.3	2011-05-31 09:58	602K	
access.log.current	2011-05-31 09:59	602K	
ftp.log	2011-05-31 09:59	383K	
ftp.log.37.gz	2011-05-31 09:59	364	
ftp.log.38.gz	2011-05-31 09:59	7.4K	
ftp.log.39.gz	2011-05-31 09:59	7.8K	
ftp.log.40.gz	2011-05-31 09:59	1.6K	
ftp.log.41.gz	2011-05-31 09:59	103K	
ftp.log.42.gz	2011-05-31 09:59	1.2K	
ftp.log.43.gz	2011-05-31 09:59	58K	
info.php	2011-05-31 10:00	21	
info.pl	2011-05-31 10:00	3.9K	
info.py	2011-05-31 10:00	6.2K	

```
Command Prompt
Microsoft Windows [Version 10.0.22000.675]
(c) Microsoft Corporation. All rights reserved.

C:\Users\dinh>echo dinhquanghieu-b19dcat065
```

- Xem thư mục backup của máy chủ ftp

exploit-db.com/ghdb/5512

EXPLOIT DATABASE

site:ftp.* index of /ftp/backup

GHDB-ID:
5512

Author:
PARAS ARORA

Published: 2019-09-10

Google Dork Description:
site:ftp.* index of /ftp/backup

Google Search: site:ftp.* index of /ftp/backup

To View *Backup* files on *FTP* server of various websites

Dork: site:ftp. index of /ftp/backup*

Author: Paras Arora(PAC Security)











Date: 9th September 2019

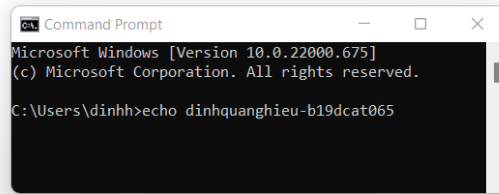
Category: Backup files on FTP Server

```
Command Prompt
Microsoft Windows [Version 10.0.22000.675]
(c) Microsoft Corporation. All rights reserved.

C:\Users\dinh>echo dinhquanghieu-b19dcat065
```

Index of /Fileshare/PDV Backup file

Name	Last modified	Size	Description
 Parent Directory		-	
 20210116/	2021-03-01 11:33	-	
 BKC/	2021-03-01 11:51	-	
 Chuc Nang Phu/	2021-03-01 11:51	-	
 Chu ky/	2021-03-01 11:51	-	
 Partner/	2021-03-01 11:51	-	
 Tieng Viet/	2021-03-01 11:51	-	
 logo.pdv/	2021-03-01 11:51	-	
 new 2.txt	2021-03-01 11:53	7.5K	
 zzz Linh Tinh/	2021-03-01 11:53	-	



```
Command Prompt
Microsoft Windows [Version 10.0.22000.675]
(c) Microsoft Corporation. All rights reserved.

C:\Users\dinh>echo dinhquanghieu-b19dcat065
```

Apache/2.4.29 (Ubuntu) Server at ftp.anphat.vn Port 80