

Báo cáo bài thực hành số 14

Môn học

Thực tập cơ sở

Giảng viên : Hoàng Xuân Dậu

Họ tên : Nguyễn Minh Phương

Mã SV: B19DCAT141

1 Lý thuyết

- 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 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)
- Google hacking
 - Google Hacking là một thuật ngữ mà gói gọn một loạt các kỹ 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 công thông tin, các loại khác nhau của các bản ghi hệ thống như tường lửa và truy cập các bản ghi....

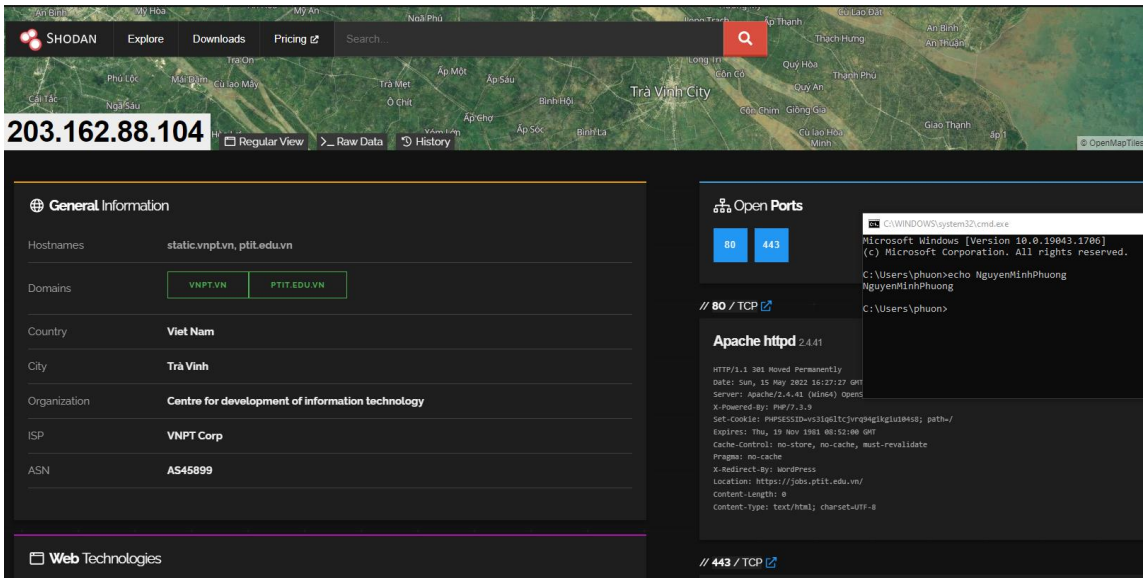
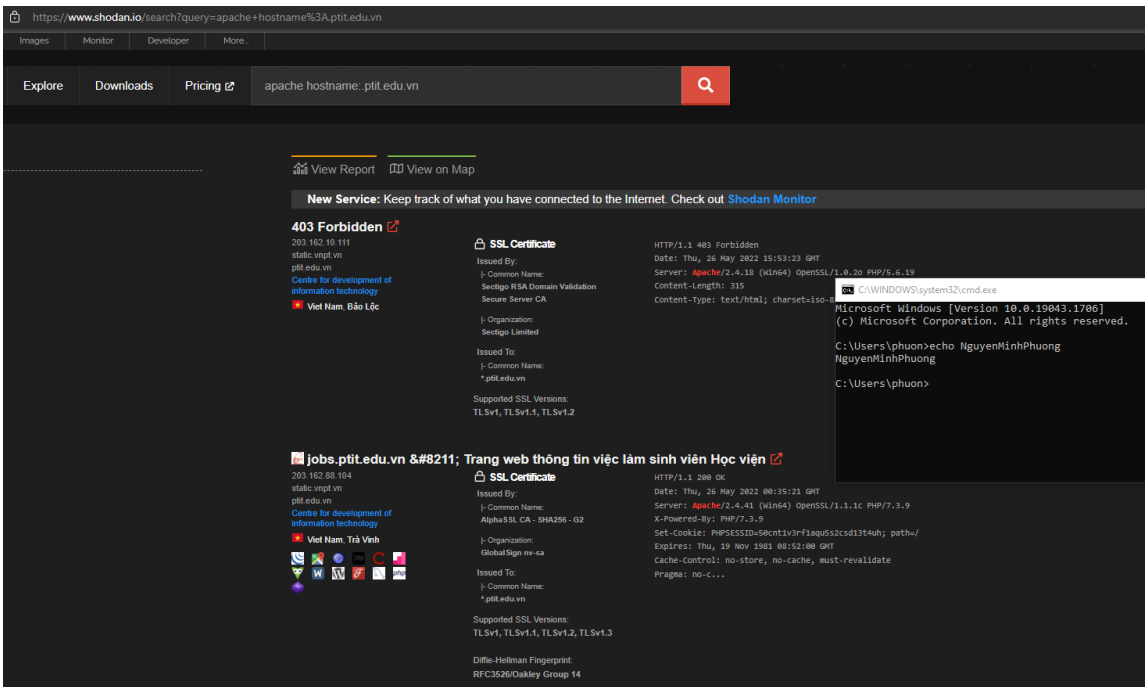
- Google hacking database chia thành nhiều loại khác nhau như: thông tin các file bị tổn thương, các file chứa mật khẩu, thông tin về máy chủ và phần mềm trên đó, tìm kiếm các thiết bị trực tuyến...etc. Một Dork chỉ là một truy vấn Google đã tìm ra kết quả hữu ích như khai thác dữ liệu nhạy cảm. Khi 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: shtm
 - 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.

2 Thực hành

Shodan

Tìm máy chủ apache và có hostname .ptit.edu.vn



Tìm máy chủ web IIS ở Hà Nội

Tìm những thiết bị chạy win 7 tại Việt Nam

The screenshot shows the Shodan search engine interface. The search query is 'os:windows 7 country:vn'. The results show 895 total results. The top cities are listed: Ho Chi Minh City (354), Hanoi (292), Da Nang (13), Bien Hoa (11), and Chi Linh (11). The top ports are listed: 3389 (672), 445 (219), and 3388 (4). The top organizations are listed: FPT Telecom, Viet Nam Hanoi, and self signed. A detailed view of a host is shown, including an SSL Certificate and Remote Desktop Protocol (RDP) information. The RDP information shows the target name as HALLE, the target IP as 118.70.128.184, and the target port as 3389. The RDP information also shows the target name as HALLE, the target IP as 118.70.128.184, and the target port as 3389. The RDP information also shows the target name as HALLE, the target IP as 118.70.128.184, and the target port as 3389.

Dùng metasploit để quét webcamxp

The screenshot shows a Metasploit Meterpreter session. The user has entered the command 'search shodan'. The output shows the following results:

#	Name	Disclosure Date	Rank	Confidence
0	auxiliary/scanner/http/influxdb_enum		normal	Normal
1	auxiliary/gather/shodan_honeyscore		normal	Normal
2	auxiliary/gather/shodan_host		normal	No
3	auxiliary/gather/shodan_search		normal	No
4	auxiliary/scanner/http/smt_ipmi_49152_exposure	2014-06-19	normal	No

The user has also entered the command 'use 3', which has loaded the 'auxiliary/dos/http/brother_debut_dos' module. The user has then entered the command 'show options', which has displayed the following options:

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type: http://proxy:port
RHOSTS		yes	The target host(s), see https://work/wiki/Using-Metasploit
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
VHOST		no	HTTP server virtual host

The screenshot shows a Metasploit Meterpreter session. The user has entered the command 'use 3', which has loaded the 'auxiliary/dos/http/brother_debut_dos' module. The user has then entered the command 'show options', which has displayed the following options:

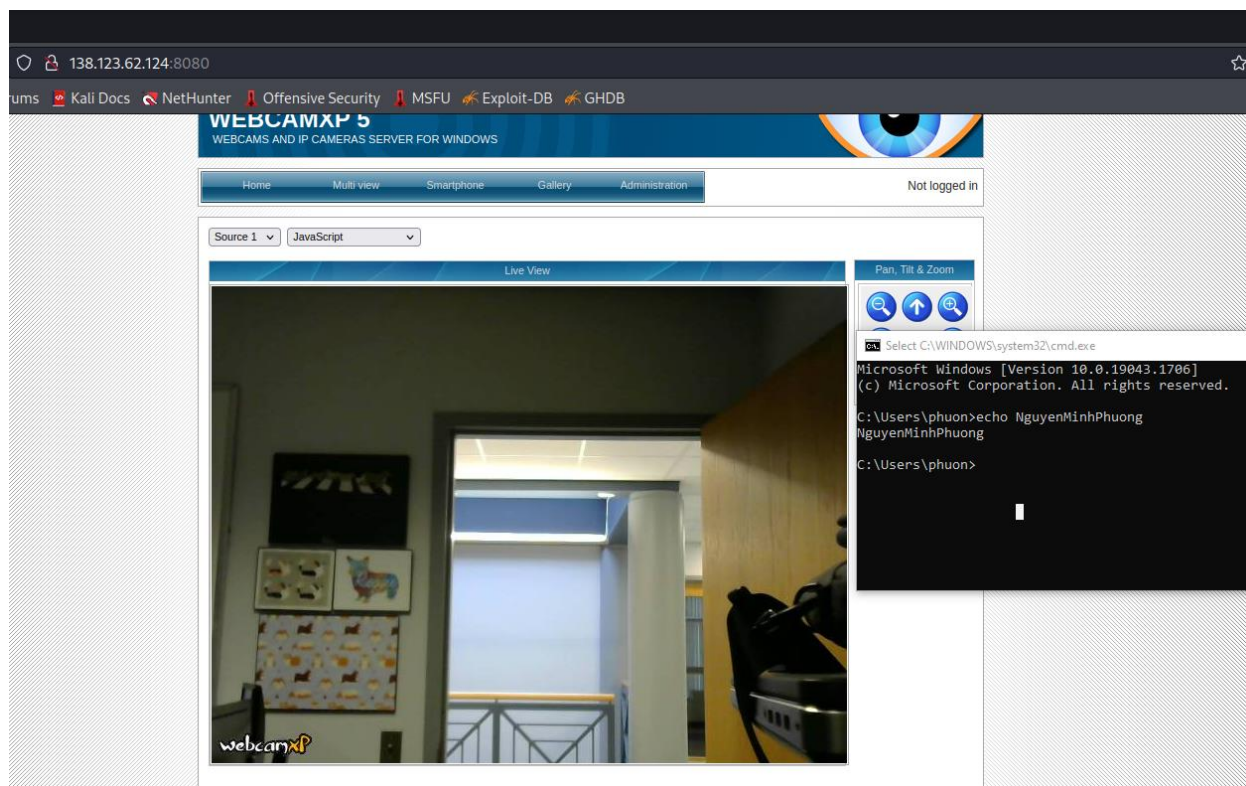
Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type: http://proxy:port
RHOSTS		yes	The target host(s), see https://work/wiki/Using-Metasploit
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
VHOST		no	HTTP server virtual host


```
Shell No. 1
File Actions Edit View Help
msf6 auxiliary(gather/shodan_search) > set shodan_apikey b6p5PJ9jKAYo
shodan_apikey => b6p5PJ9jKAYotrFrclvgso4G880Atq3e
msf6 auxiliary(gather/shodan_search) > set query webcamxp
query => webcamxp
msf6 auxiliary(gather/shodan_search) > run

[*] Total: 484 on 5 pages. Showing: 1 page(s)
[*] Collecting data, please wait ...


Search Results
```

IP:Port	City	Country	Host
1.213.178.190:20000	Seoul	Korea, Republic of	
109.254.7.27:8080	Donetsk	Ukraine	ip-
121.138.24.125:8080	Seoul	Korea, Republic of	
121.152.197.25:8080	Daejeon	Korea, Republic of	
122.117.156.176:8080	Kaohsiung	Taiwan	122-117-156-176.hinet-ip.hinet.net
125.132.184.175:1554	Seongnam-si	Korea, Republic of	
138.123.62.124:8080	Wilmington	United States	s-a228-01.dtcc.edu
139.162.119.9:80	Tokyo	Japan	li1603-9.members.linode.com
139.162.213.30:50000	London	United Kingdom	li1376-30.members.linode.com
139.162.213.30:60001	London	United Kingdom	li1376-30.members.linode.com
139.162.213.30:8888	London	United Kingdom	li1376-30.members.linode.com
139.59.122.225:80	Singapore	Singapore	
139.59.56.96:9000	Doddaballapura	India	
139.59.7.128:80	Doddaballapura	India	
14.32.190.83:8081	Seoul	Korea, Republic of	
152.86.62.9:4430	Mount Pleasant	United States	
154.127.186.9:8080	Luanda	Angola	cust9-186.127.154.tvcabo.ao
160.119.230.64:9090	Benoni	South Africa	
163.20.36.26:8080	Banqiao	Taiwan	



Google Hacking

Filter theo Vulnerable Servers



Category

Vulnerable Servers

Google Hacking Database

Show 15

Date Added # Dork

2021-11-15	inurl:adm/login.jsp.bak
2021-09-24	intitle:"TileServer GL - Server for vector and raster maps with GL styles"
2021-09-16	intitle:"index of" "/views/auth/passwords"
2021-09-08	intitle:"Icecast Streaming Media Server" "Icecast2 Status" -.com
2021-06-25	inurl /editor/filemanager/connectors/uploadtest.html
2020-12-15	intext:"user name" intext:"orion core" -solarwinds.com

Select C:\WINDOWS\system32\cmd.exe

```


Microsoft Windows [Version 10.0.19043.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\phuong>echo NguyenMinhPhuong
NguyenMinhPhuong

C:\Users\phuong>

```

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



inurl:adm/login.jsp.bak

GHDB-ID:
7782

Author:
MD ANZARUDDIN

Published: 2021-11-15

Google Dork Description:
inurl:adm/login.jsp.bak

Google Search: inurl:adm/login.jsp.bak

←

Google Dork: intitle:"R WebServer"
 # Vulnerable Server
 # Date: 12/11/2021
 # Exploit Author: Md Anzaruddin

Select C:\WINDOWS\system32\cmd.exe

```

Microsoft Windows [Version 10.0.19043.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\phuong>echo NguyenMinhPhuong
NguyenMinhPhuong

C:\Users\phuong>

```

Downloads

Certifications


Training

Kali Linux	OSCP	Penetration Testing with Kali Linux (PWK) (PEN-200) All new for 2020
Kali NetHunter	OSWP	Offensive Security Wireless Attacks (WIFU) (PEN-210)

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

EXPLOIT
DATABASE

intitle:"Index of" "DCIM"


GHDB-ID:
4057

Author:
ANONYMOUS

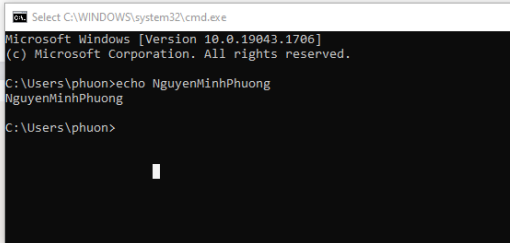
Published: 2015-08-19

Google Dork Description:
intitle:"Index of" "DCIM"

Google Search: intitle:"Index of" "DCIM"




A lot of Camera Photos Dump.
Have Fun!.
Rootkit.



Google

intitle:"Index of" "DCIM"

Tất cả Hình ảnh Video Tin tức Thêm

Công cụ

Khoảng 1.200 kết quả (0,32 giây)

<http://l3s.de/~zerr/CIKM2012/DCIM> Dịch trang này

Index of /~zerr/CIKM2012/DCIM

Index of /~zerr/CIKM2012/DCIM. [ICO], Name · Last modified · Size · Description.
[PARENTDIR], Parent Directory, -, [DIR], 100CANON/, 2012-11-29 21:57, -.

<https://ewh.ieee.org/delhi/docs/DCIM> Dịch trang này

of /sb/delhi/ggsipu/docs/lethac/videos/3/lethac pics/DCIM ...

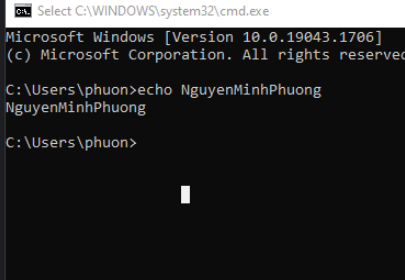
Name	Last modified	Size
Parent Directory		-
DSCN3855.JPG	2012-03-15 05:43	5.1M
DSCN3856.JPG	2012-03-15 05:43	4.0M

Xem thêm 18 hàng

















<https://www.cs.cmu.edu/~yhchu/DCIM> Dịch trang này

Index of /~yhchu/Photos/DCIM

Index of /~yhchu/Photos/DCIM. [ICO], Name · Last modified · Size · Description. [PARENTDIR],
Parent Directory, -, [DIR], 100CASIO/, 2004-06-10 23:07, - ...



Index of /~zerr/CIKM2012/DCIM/100CANON


Name	Last modified	Size	Description
 Parent Directory	-	-	-
 IMG_7530.JPG	2012-11-29 21:54	6.6M	
 IMG_7531.JPG	2012-11-29 21:48	4.6M	
 IMG_7532.JPG	2012-11-29 21:57	3.9M	
 IMG_7533.JPG	2012-11-29 21:51	4.4M	
 IMG_7534.JPG	2012-11-29 21:53	4.6M	
 IMG_7535.JPG	2012-11-29 21:55	4.0M	
 IMG_7536.JPG	2012-11-29 21:54	3.7M	
 IMG_7537.JPG	2012-11-29 21:48	4.8M	
 IMG_7538.JPG	2012-11-29 21:56	5.0M	
 IMG_7539.JPG	2012-11-29 21:53	6.1M	
 IMG_7540.JPG	2012-11-29 21:44	7.0M	
 IMG_7541.JPG	2012-11-29 21:51	6.8M	
 IMG_7542.JPG	2012-11-29 21:46	6.8M	
 IMG_7543.JPG	2012-11-29 21:48	3.8M	
 IMG_7544.JPG	2012-11-29 21:46	7.3M	

```
cmd Select C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\phuong>echo NguyenMinhPhuong
NguyenMinhPhuong

C:\Users\phuong>
```

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




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!
```

```
cmd Select C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\phuong>echo NguyenMinhPhuong
NguyenMinhPhuong

C:\Users\phuong>
```

Index of /apiAgro/puppet/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

```
cmd Select C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\phuong>echo NguyenMinhPhuong
NguyenMinhPhuong

C:\Users\phuong>
```

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.




allintext:username,password filetype:log

GHDB-ID:
6412

Author:
ISA GH0JARIA

Published: 2020-07-16

Google Dork Description:
allintext:username,password filetype:log



allintext:username,password filetype:log

```
cmd Select C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\phuong>echo NguyenMinhPhuong
NguyenMinhPhuong

C:\Users\phuong>
```

Firefox (1.x->3.x) Passwords:

```
serv - http://fr-fr.facebook.com
email      : roi_de_la_casse@hotmail.com
pass       : zzqgh9qy
-----

serv - http://fr.youtube.com
username   : Sargerans
password   : zzqgh9qy
-----

serv - http://snowtigers.net
username   : Maxter
password   : WOW071789788
-----

serv - https://login.facebook.com
email      : roi_de_la_casse@hotmail.com
pass       : zzqgh9qy
-----

serv - http://hostarea.org
login      : Sargeran
pass       : zzqgh9qy
-----

serv - http://www.facebook.com
email      : roi_de_la_casse@hotmail.com
pass       : zzqgh9qy
-----


serv - http://www.forumactif.com
:
```

```
cmd Select C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\phuong>echo NguyenMinhPhuong
NguyenMinhPhuong

C:\Users\phuong>
```

Thư mục gốc của máy chủ <ftp.riken.jp>



site:.in | .com | .net intitle:"index of" ftp


GHDB-ID:
7772

Author:
KRISHNA AGARWAL

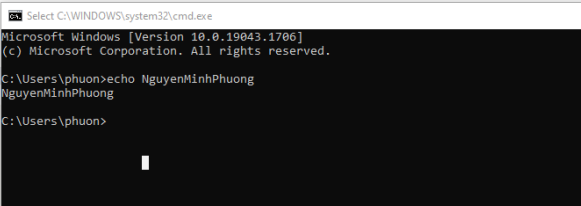
Published: 2021-11-11

Google Dork Description:
site:.in | .com | .net intitle:"index of" ftp

Google Search: site:.in | .com | .net intitle:"index of" ftp



```
# Google Dork: site:.in | .com | .net intitle:"index of" ftp
# Files Containing Juicy Info
# Date:11/11/2021
# Exploit Author: Krishna Agarwal
```









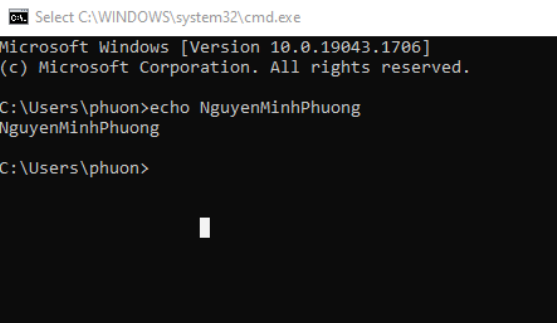
```
Select C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\phuong>echo NguyenMinhPhuong
NguyenMinhPhuong

C:\Users\phuong>
```

Index of /net

Name	Last modified	Size	Description
 Parent Directory		-	
 OpenSSL/	2022-05-27 14:41	-	
 ProFTPD/	2022-05-27 02:45	-	
 apache/	2022-05-27 19:32	-	
 postfix-release/	2022-02-05 03:00	-	
 postfix/	2017-06-29 22:16	-	
 samba/	2020-03-02 11:35	-	




```
Select C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\phuong>echo NguyenMinhPhuong
NguyenMinhPhuong

C:\Users\phuong>
```

Xem các file log của máy chủ ftp



intitle:"index of" "ftp.log"


GHDB-ID:
5716

Author:
PANKAJ KUMAR THAKUR

Published: 2020-01-28

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

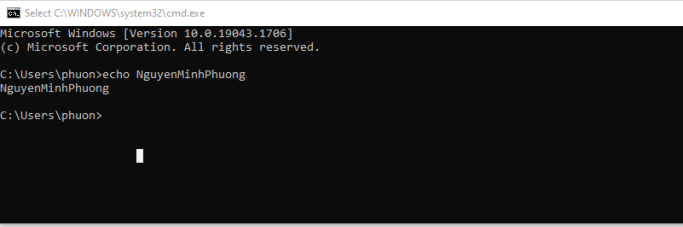
Google Search: intitle:"index of" "ftp.log"



```
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
```



```
Select C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\phuong>echo NguyenMinhPhuong
NguyenMinhPhuong

C:\Users\phuong>
```

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	

```
CA: Select C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\phuong>echo NguyenMinhPhuong
NguyenMinhPhuong

C:\Users\phuong>
```

Xem thư mục backup của máy chủ ftp



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

```
CA: Select C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\phuong>echo NguyenMinhPhuong
NguyenMinhPhuong

C:\Users\phuong>
```

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	-	-
Tiem 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	-	-

```
CA: Select C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\phuong>echo NguyenMinhPhuong
NguyenMinhPhuong

C:\Users\phuong>
```

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