

BÁO CÁO BÀI TẬP

Môn học: An Toàn Mạng

Tên chủ đề: Information Gathering

GVHD: Ngô Đức Hoàng Sơn

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT140.011.ATCL

STT	Họ và tên	MSSV	Email
1	Dương Phan Hiếu Nghĩa	21521179	21521179@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Câu 1-35:	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1.

MegaCorp One là công ty hoạt động trong lĩnh vực công nghệ nano. Chịu trách nhiệm xác định các tiêu chuẩn của ngành trong lĩnh vực y tế, điện tử và thương mại.

About Us

MegaCorp One specializes in **disruptive innovation** in the nanotechnology industry. We are responsible for industry defining standards in the medical, electronic, and commerce fields.

Our success begins with the assessment of small teams working on independent project. Once we have selected a project that we believe will succeed, we procure their talent and refine the technology toward our common goals.

The ability to discover and encourage the brightest minds in the industry, has led to our rapidly increasing growth.

Chief Executive Officer, Joe Sheer, has been featured in the Journal of NanoTimes stating:

2.

Đội ngũ điều hành gồm

- + Joe Sheer (CEO): joe@megacorpone.com
- + Mike Carlow (VP Of Legal): mcarlow@megacorpone.com
- + Anlan Brofielf (IT and Security Director): agrofield@megacorpone.com
- + Matt Smith (Marketing Director): msmith@megacorpone.com



Joe Sheer

**CHIEF EXECUTIVE
OFFICER**

Email:
joe@megacorpone.com

Twitter: [@Joe_Sheer](https://twitter.com/Joe_Sheer)



Tom Hudson

WEB DESIGNER

Email: thudson@megacorpone.com

Twitter:
[@TomHudsonMCO](https://twitter.com/TomHudsonMCO)



Tanya Rivera

SENIOR DEVELOPER

Email:
trivera@megacorpone.com

Twitter:
[@TanyaRiveraMCO](https://twitter.com/TanyaRiveraMCO)



Matt Smith

**MARKETING
DIRECTOR**

Email:
msmith@megacorpone.com

Twitter:
[@MattSmithMCO](https://twitter.com/MattSmithMCO)

Hình 1.

3.

Địa chỉ email của họ có cùng tên miền “megacorpone.com” cho thấy rằng họ đều thuộc về cùng một công ty Megacorp One.

4.

```
$ whois NS1.MEGACORPONE.COM
Server Name: NS1.MEGACORPONE.COM
IP Address: 51.79.37.18
Registrar: Gandi SAS
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Last update of whois database: 2023-10-14T04:23:27Z <<<
```

Hình 2.

```
$ whois NS2.MEGACORPONE.COM
Server Name: NS2.MEGACORPONE.COM
IP Address: 51.222.39.63
Registrar: Gandi SAS
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
>> Last update of whois database: 2023-10-14T04:24:27Z <<<
```

Hình 3.

```
$ whois NS3.MEGACORPONE.COM
Server Name: NS3.MEGACORPONE.COM
IP Address: 66.70.207.180
Registrar: Gandi SAS
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
>>> Last update of whois database: 2023-10-14T04:24:58Z <<<
```

Hình 4.

5.

```
$ whois uit.edu.vn
This TLD has no whois server, but you can access the whois database at
http://www.vnnic.vn/en
```

Không thể dùng whois để xem thông tin uit.edu.vn

Vì tên miền uit.edu.vn sử dụng một TLD không hỗ trợ truy cập thông tin thông qua WHOIS.

-> Ta phải sử dụng trang web của VNNIC để tra cứu thông tin vì tên miền này do cơ quan quản lý tên miền quốc gia Việt Nam quản lý.

6.

- Ngày đăng ký tên miền: 2006-10-02
- Ngày hết hạn tên miền: 2024-10-02
- Chủ sở hữu tên miền: Trường Đại học Công nghệ Thông tin
- Các nameserver của tên miền:
 - ns1.pavietnam.vn
 - ns2.pavietnam.vn
 - nsbak.pavietnam.net

Domain Name:	uit.edu.vn
Registrant Name:	Trường Đại học Công nghệ Thông tin
Registrar:	Công ty TNHH PA Việt Nam
Creation Date:	2006-10-02
Expiration Date:	2024-10-02
Status:	clientTransferProhibited
Nameserver:	ns1.pavietnam.vn ns2.pavietnam.vn nsbak.pavietnam.net

Hình 5.

7.

Phó chủ tịch Pháp lý (Vice President of Legal) của MegaCorp One là
Mike Carlow

Địa chỉ email: mcarlow@megacorpone.com

Name: Mike Carlow


Title: VP Of Legal



Email: mcarlow@megacorpone.com

Hình 6.

8. Tra cứu tại: <https://www.zoominfo.com/pic/megacorp-one/1160818919>

Index of contact profiles from MegaCorp One


Contact Name  Stan Denvers



Contact Info  Email  Direct

Job Title Collections

Location United States, Nevada, Rachel

Last Update 10/8/2023


Contact Name  Alan Grofield



Contact Info  Email  Direct

Job Title —

Location United States, Nevada, Rachel

Last Update 10/7/2023


Contact Name  Steve Wong



Contact Info  Email  Direct

Job Title System Administrator

Location United States, Nevada, Rachel

Last Update 10/7/2023

Contact Name  Tom Hudson

Contact Info  Email  Direct

Job Title Web Designer

Location United States, Nevada, Rachel

Last Update 10/7/2023


Contact Name  Johnny Five



Contact Info  Email  Direct

Job Title —

Location United States, Nevada, Rachel

Last Update 10/7/2023

Contact Name  Handy McKay

Contact Info  Email  Direct

Job Title —

Location United States, Nevada, Rachel

Last Update 10/7/2023

Hình 7.

9.

Filetype: tìm kiếm tệp tin cụ thể theo loại tệp tin

filetype:pdf google hacking

site: hạn chế kết quả tìm kiếm cho một trang web cụ thể

site:wikipedia.org artificial intelligence

intitle: tìm kiếm từ khóa xuất hiện trong tiêu đề của trang web

intitle:"cyber security"

inurl: tìm kiếm từ khóa xuất hiện trong url của trang web

inurl:admin login

cache: tìm bản sao lưu của trang web được lưu trong bộ nhớ đệm của Google

cache:uit.edu.vn

10.

- Email của lớp có dạng: <tên lớp>@gm.uit.edu.vn. Ví dụ: một thành viên của lớp Kỹ thuật Phần mềm Khóa 2021 gửi email vào địa chỉ của lớp mình đang sinh hoạt là: ktpm2021@gm.uit.edu.vn thì email này sẽ được gửi đến các thành viên khác trong lớp, cố vấn học tập và đơn vị quản lý sinh viên.

Hình 8.

Đây là thông tin có thể dễ dàng được xem bởi bất kỳ ai trên mạng internet tại địa chỉ <https://ctsv.uit.edu.vn/bai-viet/quan-ly-thong-tin-sinh-vien>



Theo em nó nên giới hạn chỉ sinh viên được xem, tránh những cá nhân có ý định xấu sẽ gửi nhưng mail spam, chứa thông tin lừa đảo, độc hại cho nhiều sinh viên. Mã lớp là thông tin dễ tìm được trên internet nên việc biết được mail của có là dễ dàng.

Thông tin mã lớp có thể lấy được: <https://ctsv.uit.edu.vn/bai-viet/khoa-hoc-lop-sinh-vien-thoi-gian-tiet-hoc>

11.

Application Servers

An application server is a server that provides software applications with services such as security, data services, transaction support, load balancing, and management of large distributed systems.

Technology	Description	Popular sites using this technology
Apache 	Web server software	www.24presse.com , www.calculator.net , www.smtpcorp.com
Debian 	No description	www.hhv.de , www.francesoir.fr , www.majorgeeks.com

Máy chủ Apache

Hệ điều hành Debian

12.

Dùng modules hackertarget

```
[recon-ng][default] > modules load recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > options set SOURCE megacorpone.com
SOURCE ⇒ megacorpone.com
[recon-ng][default][hackertarget] > run

MEGACORPONE.COM

[*] Country: None
[*] Host: fs1.megacorpone.com
[*] Ip_Address: 51.222.169.210
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: ns1.megacorpone.com
[*] Ip_Address: 51.79.37.18
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: mail2.megacorpone.com
[*] Ip_Address: 51.222.169.213
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: ns2.megacorpone.com
[*] Ip_Address: 51.222.39.63
```

Kết quả:


```
[recon-ng][default] > show hosts
```

rowid	host	ip_address	region	country	latitude	longitude	notes	module
1	www.megacorpone.com							google_site_web
2	fs1.megacorpone.com	51.222.169.210						hackertarget
3	ns1.megacorpone.com	51.79.37.18						hackertarget
4	mail2.megacorpone.com	51.222.169.213						hackertarget
5	ns2.megacorpone.com	51.222.39.63						hackertarget
6	www2.megacorpone.com	149.56.244.87						hackertarget
7	ns3.megacorpone.com	66.70.207.180						hackertarget
8	beta.megacorpone.com	51.222.169.209						hackertarget
9	syslog.megacorpone.com	51.222.169.217						hackertarget
10	mail.megacorpone.com	51.222.169.212						hackertarget
11	siem.megacorpone.com	51.222.169.215						hackertarget
12	admin.megacorpone.com	51.222.169.208						hackertarget
13	vpn.megacorpone.com	51.222.169.220						hackertarget
14	snmp.megacorpone.com	51.222.169.216						hackertarget
15	router.megacorpone.com	51.222.169.214						hackertarget
16	intranet.megacorpone.com	51.222.169.211						hackertarget
17	support.megacorpone.com	51.222.169.218						hackertarget
18	test.megacorpone.com	51.222.169.219						hackertarget
19	www.megacorpone.com	149.56.244.87						hackertarget

13.

Thu thập thông tin về UIT:

20	mx1.uit.edu.vn			45.122.249.78				hackertarget
21	mapr2022.uit.edu.vn			118.69.123.140				hackertarget
22	a084742fa316491c8c78564efcbce9e0-68f6236f-vm-80.vlab2.uit.edu.vn			45.122.249.76				hackertarget
23	host2.uit.edu.vn			45.122.249.78				hackertarget
24	mx2.uit.edu.vn			45.122.249.78				hackertarget
25	forum4.uit.edu.vn			45.122.249.78				hackertarget
26	sois2017.uit.edu.vn			45.122.249.78				hackertarget
27	mapr2018.uit.edu.vn			45.122.249.78				hackertarget
28	daa.uit.edu.vn			118.69.123.140				hackertarget
29	mitaka.uit.edu.vn			45.122.249.78				hackertarget
30	forumbeta.uit.edu.vn			118.69.123.140				hackertarget
31	inseclab.uit.edu.vn			118.69.123.140				hackertarget
32	api.mmlab.uit.edu.vn			118.69.123.142				hackertarget
33	annotation.mmlab.uit.edu.vn			118.69.123.142				hackertarget
34	demo.mmlab.uit.edu.vn			42.116.11.23				hackertarget
35	vlab.uit.edu.vn			45.122.249.74				hackertarget
36	519bb137df6144dcbeda18e87d53ad8a-0-s-80.vlab.uit.edu.vn			45.122.249.74				hackertarget
37	console-cloud.vlab.uit.edu.vn			45.122.249.74				hackertarget
38	qttb.uit.edu.vn			118.69.123.140				hackertarget
39	isccclub.uit.edu.vn			118.69.123.140				hackertarget
40	aiclub.uit.edu.vn			118.69.123.140				hackertarget
41	qlhc.uit.edu.vn			45.122.249.78				hackertarget
42	nc.uit.edu.vn			45.122.249.78				hackertarget
43	dsc.uit.edu.vn			118.69.123.140				hackertarget
44	cns.uit.edu.vn			118.69.123.140				hackertarget
45	khtc.uit.edu.vn			118.69.123.140				hackertarget
46	chungthuc.uit.edu.vn			118.69.123.140				hackertarget
47	cd.uit.edu.vn			45.122.249.78				hackertarget
48	tech4covid.uit.edu.vn			45.122.249.78				hackertarget
49	hcmccovidsafe.tech4covid.uit.edu.vn			118.69.123.140				hackertarget
50	hcmccovidsafe-dev.tech4covid.uit.edu.vn			45.122.249.78				hackertarget
51	gw.tech4covid.uit.edu.vn			45.122.249.78				hackertarget
52	hcmccovidsafe-gw.tech4covid.uit.edu.vn			118.69.123.140				hackertarget
53	fce.uit.edu.vn			118.69.123.140				hackertarget
54	ecommerce.uit.edu.vn			118.69.123.140				hackertarget
55	khoahoctre.uit.edu.vn			118.69.123.140				hackertarget
56	se.uit.edu.vn			118.69.123.140				hackertarget
57	esetupdate.uit.edu.vn			118.69.123.142				hackertarget
58	live.uit.edu.vn			42.116.11.16				hackertarget
59	extensivereading.uit.edu.vn			118.69.123.140				hackertarget
60	elearning.uit.edu.vn			118.69.123.140				hackertarget
61	huongnghiepdhag.uit.edu.vn			45.122.249.78				hackertarget
62	sdh.uit.edu.vn			118.69.123.140				hackertarget
63	tuyensinh.uit.edu.vn			118.69.123.140				hackertarget
64	auth.uit.edu.vn			118.69.123.140				hackertarget
65	openstack.uit.edu.vn			118.69.123.140				hackertarget
66	link.uit.edu.vn			118.69.123.140				hackertarget
67	notebook.uit.edu.vn			118.69.123.140				hackertarget
68	dreamspark.uit.edu.vn			118.69.123.140				hackertarget
69	portal.uit.edu.vn			45.122.249.78				hackertarget
70	dbcl.uit.edu.vn			118.69.123.140				hackertarget
71	phongdl.uit.edu.vn			118.69.123.140				hackertarget
72	bandl.uit.edu.vn			118.69.123.140				hackertarget
73	congdoanql.uit.edu.vn			45.122.249.78				hackertarget
74	acm.uit.edu.vn			45.122.249.78				hackertarget
75	tracnghiem.uit.edu.vn			45.122.249.78				hackertarget
76	forum.uit.edu.vn			45.122.249.78				hackertarget
77	debian.uit.edu.vn			118.69.123.140				hackertarget
78	congdoan.uit.edu.vn			118.69.123.140				hackertarget
79	khcn.uit.edu.vn			118.69.123.140				hackertarget
80	qhdn.uit.edu.vn			45.122.249.78				hackertarget
81	en.uit.edu.vn			45.122.249.78				hackertarget
82	thuvien.uit.edu.vn			45.122.249.78				hackertarget
83	www.thuvien.uit.edu.vn			118.69.123.140				hackertarget
84	cybertrain.uit.edu.vn			118.69.123.140				hackertarget
85	doantn.uit.edu.vn			118.69.123.140				hackertarget
86	dangbo.uit.edu.vn			118.69.123.140				hackertarget
87	huongnghiep.uit.edu.vn			118.69.123.140				hackertarget
88	oep.uit.edu.vn			45.122.249.78				hackertarget
89	demodkhp.uit.edu.vn			45.122.249.78				hackertarget

90	nlp.uit.edu.vn	45.122.249.78	hackertarget
91	ftp.uit.edu.vn	42.116.6.44	hackertarget
92	hostmaster.uit.edu.vn	45.122.249.78	hackertarget
93	mapr.uit.edu.vn	118.69.123.140	hackertarget
94	sonaas.uit.edu.vn	118.69.123.140	hackertarget
95	cs.uit.edu.vn	45.122.249.78	hackertarget
96	aiclub.cs.uit.edu.vn	118.69.123.140	hackertarget
97	service.aiclub.cs.uit.edu.vn	45.122.249.78	hackertarget
98	student.cs.uit.edu.vn	118.69.123.140	hackertarget
99	banqlcs.uit.edu.vn	45.122.249.78	hackertarget
100	courses.uit.edu.vn	118.69.123.140	hackertarget
101	oms.uit.edu.vn	118.69.123.140	hackertarget
102	netsens.uit.edu.vn	45.122.249.78	hackertarget
103	photos.uit.edu.vn	45.122.249.78	hackertarget
104	qltd.uit.edu.vn	118.69.123.140	hackertarget
105	eset.uit.edu.vn	118.69.123.140	hackertarget
106	ctgt.uit.edu.vn	118.69.123.140	hackertarget
107	fit.uit.edu.vn	118.69.123.140	hackertarget
108	git.uit.edu.vn	118.69.123.138	hackertarget
109	khmt.uit.edu.vn	118.69.123.140	hackertarget
110	mmt.uit.edu.vn	45.122.249.78	hackertarget
111	ktmt.uit.edu.vn	118.69.123.140	hackertarget
112	student.uit.edu.vn	118.69.123.140	hackertarget
113	iot.uit.edu.vn	45.122.249.78	hackertarget
114	appl.iot.uit.edu.vn	45.122.249.78	hackertarget
115	testbed.iot.uit.edu.vn	118.69.123.140	hackertarget
116	forum.iot.uit.edu.vn	118.69.123.140	hackertarget
117	http.uit.edu.vn	118.69.123.140	hackertarget
118	ecommerce.http.uit.edu.vn	118.69.123.140	hackertarget
119	ptnhttp.uit.edu.vn	45.122.249.78	hackertarget
120	ctsv.uit.edu.vn	45.122.249.78	hackertarget
121	www.uit.edu.vn	118.69.123.140	hackertarget
122	ceday.uit.edu.vn	118.69.123.140	hackertarget
123	danguy.uit.edu.vn	45.122.249.78	hackertarget

14.

Kiểm tra code store-pattern của uifers: <https://github.com/uifers/store-pattern>

Dùng gitleaks phát hiện 1 lỗi:

```
(kali㉿kali)-[~/Desktop/NetworkSecurity]
$ gitleaks detect --source store-pattern --report-path report.json

O
|
O
|
O
|
gitleaks

3:58AM INF 210 commits scanned.
3:58AM INF scan completed in 4.15s
3:58AM WRN leaks found: 1
```

Lỗi Generic API Key


```

report.json
File Edit Search Options Help
[
{
  "Description": "Generic API Key",
  "StartLine": 13,
  "EndLine": 13,
  "StartColumn": 10,
  "EndColumn": 83,
  "Match": "token = '71140d8cfef118324a2fa9218b958c6f02b5f83e6810fb8c665f0cd7ef919043'",
  "Secret": "71140d8cfef118324a2fa9218b958c6f02b5f83e6810fb8c665f0cd7ef919043",
  "File": "order_app/lib/Models/connectServer.dart",
  "SymlinkFile": "",
  "Commit": "661c1dd91697df34ace1441c77d71ce9fa341e45",
  "Entropy": 3.864265,
  "Author": "yeutham212",
  "Email": "meomeocf98@gmail.com",
  "Date": "2018-11-21T17:12:57Z",
  "Message": "Update MySqlConnection",
  "Tags": [],
  "RuleID": "generic-api-key",
  "Fingerprint": "661c1dd91697df34ace1441c77d71ce9fa341e45:order_app/lib/Models/connectServer
}
]

```

15.

Thêm từ khóa webcam và city để xem các thiết bị webcam ở tại thành phố mong muốn.

The screenshot shows the Shodan search interface. The search query is 'webcam city:Ho Chi Minh'. The results show 2 total results. The top results are for IP addresses 171.244.37.108, which are associated with Viettel Group and Nam Ho Chi Minh City. The results include details such as HTTP status (200 OK), X-Powered-By (Express), Accept-Ranges (bytes), Cache-Control (public, max-age=0), Last-Modified (Tue, 31 Jan 2023 04:22:47 GMT), ETag (W/"38af-186061026ff"), Content-Type (text/html; charset=UTF-8), Content-Length (14511), Date (Mon, 23 Oct 2023 19:39:03 GMT), and Connection (keep-alive).

Tìm kiếm các máy chủ dùng hệ điều hành Linux và có CVE

16.

- + Shodan: tập trung tìm kiếm thông tin về các thiết bị và máy chủ được kết nối trực tiếp với Internet, bao gồm các máy chủ web, router, thiết bị IoT và nhiều thiết bị khác.

- Loại thông tin:

- + Bing và Google: tìm kiếm nội dung trên trang web, văn bản, hình ảnh, video và các tài liệu.

- Quyền riêng tư và bảo mật:
 - + Shodan: tuân thủ quy định và luật pháp về quyền riêng tư và bảo mật.
 - + Google và Bing: tìm kiếm nội dung công khai.
- Mục đích sử dụng:
 - + Shodan: thường được sử dụng bởi các chuyên gia bảo mật mạng và nhà nghiên cứu bảo mật để tìm kiếm và theo dõi cơ sở hạ tầng mạng trực tuyến.
 - + Bing và Google: phục vụ tìm kiếm thông tin chung, tra cứu, nghiên cứu.

17.

```
(root@kali)-[~]  
# theHarvester -d gm.uit.edu.vn -b all
```

```
[*] Emails found: 92
01234567@gm.uit.edu.vn
08520049@gm.uit.edu.vn
08520594@gm.uit.edu.vn
09520038@gm.uit.edu.vn
09520223@gm.uit.edu.vn
09520246@gm.uit.edu.vn
09520567@gm.uit.edu.vn
09520657@gm.uit.edu.vn
1,15520825@gm.uit.edu.vn
10520004@gm.uit.edu.vn
10520023@gm.uit.edu.vn
10520026@gm.uit.edu.vn
10520027@gm.uit.edu.vn
10520032@gm.uit.edu.vn
10520261@gm.uit.edu.vn
10520636@gm.uit.edu.vn
11520218@gm.uit.edu.vn
11520481@gm.uit.edu.vn
11520507@gm.uit.edu.vn
12345678@gm.uit.edu.vn
123456@gm.uit.edu.vn
12520248@gm.uit.edu.vn
12520365@gm.uit.edu.vn
12520484@gm.uit.edu.vn
12520494@gm.uit.edu.vn
13520466@gm.uit.edu.vn
13520513@gm.uit.edu.vn
14520165@gm.uit.edu.vn
14520742@gm.uit.edu.vn
14520759@gm.uit.edu.vn
14520768@gm.uit.edu.vn
14520771@gm.uit.edu.vn
14520777@gm.uit.edu.vn
15520035@gm.uit.edu.vn
15520180@gm.uit.edu.vn
15520241@gm.uit.edu.vn
15520743@gm.uit.edu.vn
15520983@gm.uit.edu.vn
16520196@gm.uit.edu.vn
16520259@gm.uit.edu.vn
16520339@gm.uit.edu.vn
16520354@gm.uit.edu.vn
16520395@gm.uit.edu.vn
16520803@gm.uit.edu.vn
16520896@gm.uit.edu.vn
```

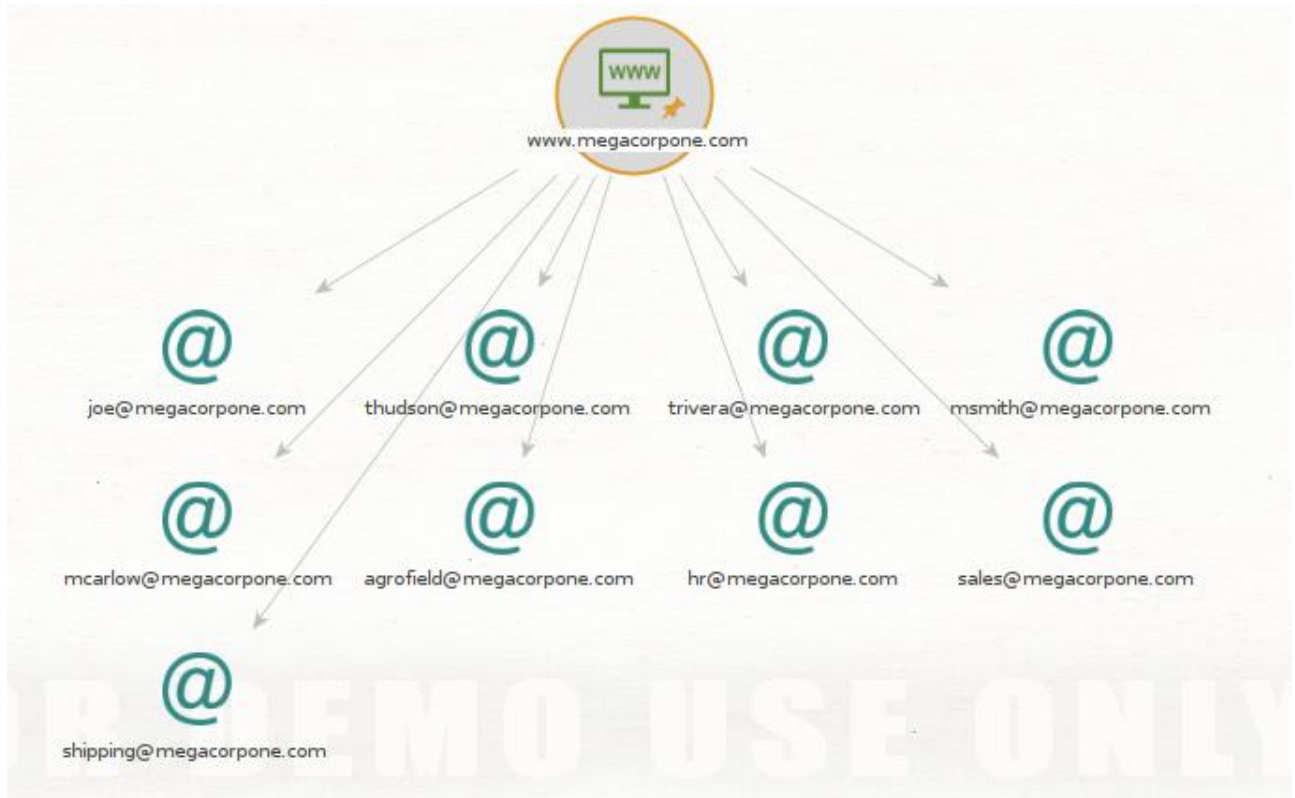
18.

Tìm với bing:

```
(kali㉿kali)-[~/Desktop/NetworkSecurity]
$ theHarvester -d uit.edu.vn -b bing
*****
*                               *
* [theHarvester]                *
*                               *
*                               *
* theHarvester 4.2.0            *
* Coded by Christian Martorella *
* Edge-Security Research       *
* cmartorella@edge-security.com *
*                               *
*                               *
*                               *
[*] Target: uit.edu.vn
^[[A Searching 0 results.
[*] Searching Bing.
[*] No IPs found.
[*] Emails found: 2
info@uit.edu.vn
phongdaotaodh@uit.edu.vn
```

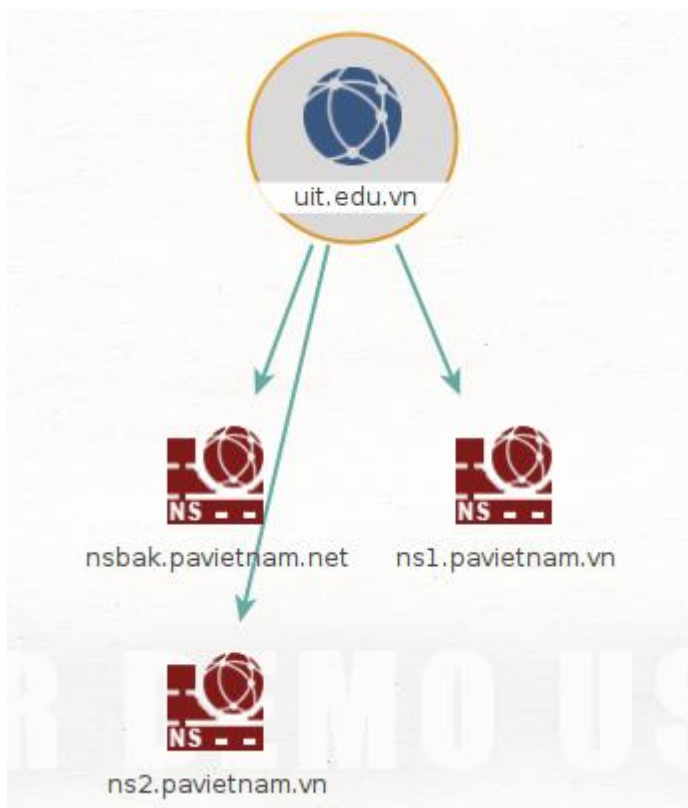
-> Sử dụng all tốt hơn vì có thể tìm tất cả các nguồn, được nhiều thông tin hơn.

19.

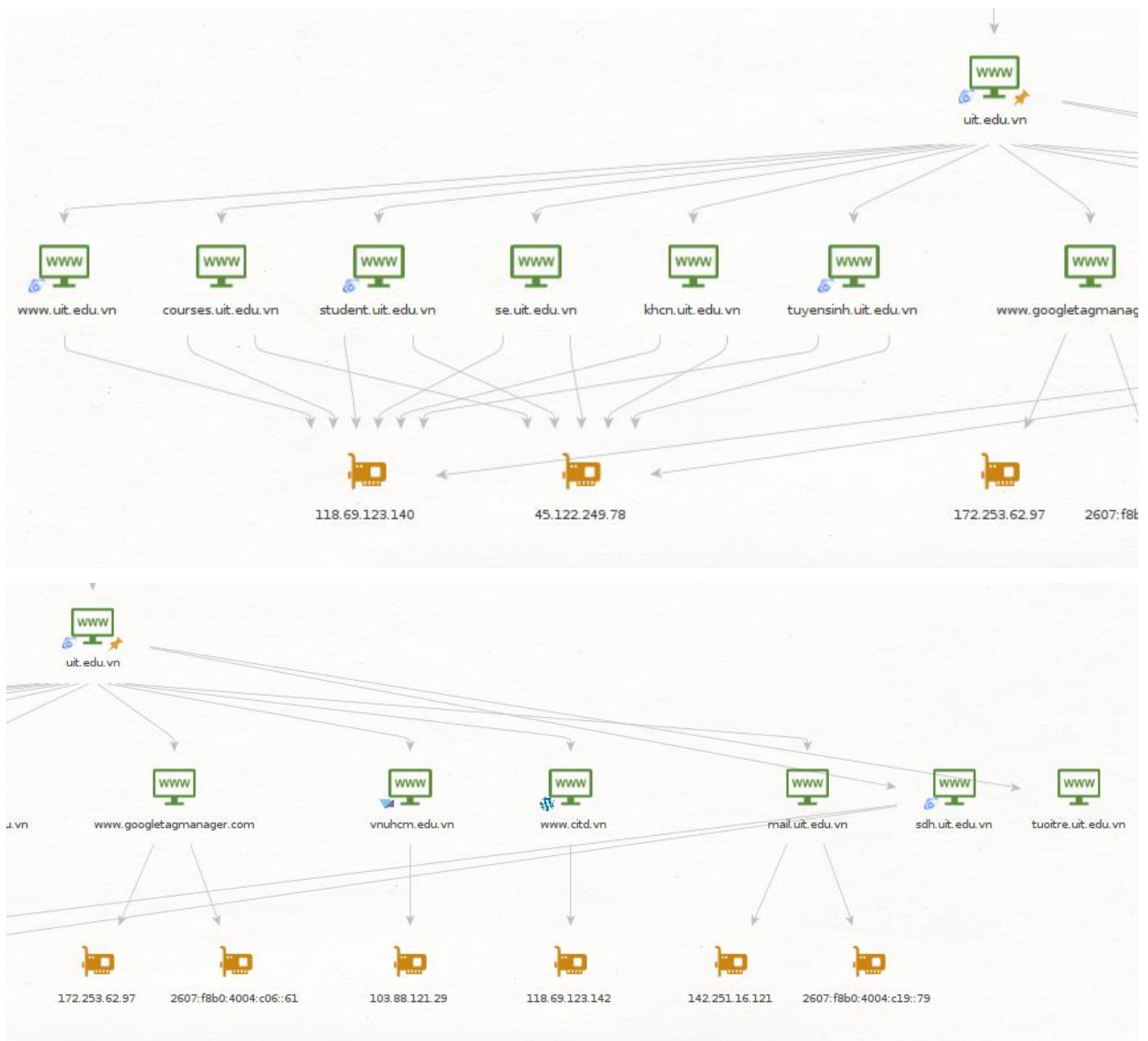


20.

a.



b)



21.

- Bản ghi AAAA (IPv6 Address Record): ánh xạ tên miền thành địa chỉ IPv6
- Bản ghi SRV (Server Record): xác định dịch vụ và máy chủ cung cấp dịch vụ cho tên miền
- Bản ghi SOA (Start of Authority Record): xác định máy chủ chịu trách nhiệm quản lý dữ liệu DNS cho một tên miền. Nó cũng chứa các thông tin quản trị tên miền.
- Bản ghi SPF (Sender Policy Framework): thông tin về các máy chủ được phép gửi mail thay mặt cho tên miền, giúp xác định email có nguồn gốc từ 1 nguồn đáng tin cậy.
- Bản ghi DKIM (DomainKeys Identified Mail): sử dụng để chữ ký số các email gửi từ tên miền, giúp xác thực email và đảm bảo tính toàn vẹn của nội dung.
- Bản ghi TLSA (TLS Authentication): xác định chứng chỉ TLS/SSL mà máy chủ sử dụng để bảo mật kết nối.
- Bản ghi LOC (Location Record): thông tin địa lý của máy chủ dựa trên tọa độ địa lý.

- Bản ghi MXE (Mail Exchange Enhanced Record): giống MX nhưng đi kèm các thông tin bổ sung về độ ưu tiên của máy chủ email.

22.

```
(kali㉿kali)-[~]
$ host -t mx uit.edu.vn
uit.edu.vn mail is handled by 40 aspmx3.googlemail.com.
uit.edu.vn mail is handled by 20 alt2.aspmx.l.google.com.
uit.edu.vn mail is handled by 10 aspmx.l.google.com.
uit.edu.vn mail is handled by 40 aspmx2.googlemail.com.
uit.edu.vn mail is handled by 20 alt1.aspmx.l.google.com.

(kali㉿kali)-[~]
$ host -t txt uit.edu.vn
uit.edu.vn descriptive text "svp60rjlr6s19rn9t013cfwm3xmox7h"
uit.edu.vn descriptive text "sqm6y27vn74pm290pl0fq4hcr08gst5r"
uit.edu.vn descriptive text "google-site-verification=wjArKGa37oHK083XqT2C91tPny8NLttGS0aU5p"
uit.edu.vn descriptive text "MS=E431E3CA3EFF5A6431E2378C924984A8A0334ABC"
uit.edu.vn descriptive text "v=spf1 include:_spf.google.com ~all"
```

Hình 9.

23.

```
(kali㉿kali)-[~]
$ host idontexist.uit.edu.vn
idontexist.uit.edu.vn has address 45.122.249.78
idontexist.uit.edu.vn has address 118.69.123.140

(kali㉿kali)-[~]
$ host noexits.idontexist.uit.edu.vn
noexits.idontexist.uit.edu.vn has address 45.122.249.78
noexits.idontexist.uit.edu.vn has address 118.69.123.140

(kali㉿kali)-[~]
$ host baithuchanhso2.noexits.idontexist.uit.edu.vn
baithuchanhso2.noexits.idontexist.uit.edu.vn has address 45.122.249.78
baithuchanhso2.noexits.idontexist.uit.edu.vn has address 118.69.123.140
```

Hình 10.

Các hostname không tồn tại đều có cùng địa chỉ IP. Khi tìm kiếm 1 hostname không tồn tại hệ thống DNS sẽ trả về địa chỉ IP mặc định, giúp tránh các lỗ hổng bảo mật.

24.

Dùng wordlist seclists, loại bỏ các kết quả fail:

```
(kali㉿kali)-[~/Desktop]
$ for ip in $(cat common.txt); do
  result=$(host $ip.megacorpone.com)
  if [[ $result != *NXDOMAIN* ]]; then
    echo $result
  fi
done
```

Hình 11.

➔ Kết quả brute force:

```

admin.megacorpone.com has address 51.222.169.208
beta.megacorpone.com has address 51.222.169.209
fs1.megacorpone.com has address 51.222.169.210
intranet.megacorpone.com has address 51.222.169.211
mail.megacorpone.com has address 51.222.169.212
mail2.megacorpone.com has address 51.222.169.213
ns1.megacorpone.com has address 51.79.37.18
ns2.megacorpone.com has address 51.222.39.63
ns3.megacorpone.com has address 66.70.207.180
router.megacorpone.com has address 51.222.169.214
siem.megacorpone.com has address 51.222.169.215
snmp.megacorpone.com has address 51.222.169.216
support.megacorpone.com has address 51.222.169.218
syslog.megacorpone.com has address 51.222.169.217
test.megacorpone.com has address 51.222.169.219
vpn.megacorpone.com has address 51.222.169.220
www.megacorpone.com has address 149.56.244.87
www2.megacorpone.com has address 149.56.244.87

```

Hình 12.

25.

Đoạn script bash shell:

```

1 #!/bin/bash
2
3 hcmus=("dns2.hcmus.edu.vn" "dns1.hcmus.edu.vn" "server.hcmus.edu.vn")
4 hcmussh=("server.vnuhcm.edu.vn" "vnuserv.vnuhcm.edu.vn")
5 uit=("nsbak.pavietnam.net" "ns1.pavietnam.vn" "ns2.pavietnam.vn")
6 hcmut=("dns3.hcmut.edu.vn" "dns2.hcmut.edu.vn" "dns4.hcmut.edu.vn" "dns1.hcmut.edu.vn")
7 hcmiu=("hcm-server1.vnn.vn" "vdc-hn01.vnn.vn")
8 uel=("ns1.dns.net.vn" "ns2.dns.net.vn")
9 hcmier=("server.vnuhcm.edu.vn" "vnuserv.vnuhcm.edu.vn")
10 vnuhcm=("server.vnuhcm.edu.vn" "vnuserv.vnuhcm.edu.vn" "ns2.vdc2.vn" "ns1.vdc2.vn")
11
12 echo "hcmus:"
13 for ns in "${hcmus[@]}"; do
14     host -l hcmus.edu.vn "$ns"
15 done
16
17 echo "/nhcmussh:"
18 for ns in "${hcmussh[@]}"; do
19     host -l hcmussh.edu.vn "$ns"
20 done
21
22 echo "/nuit:"
23 for ns in "${uit[@]}"; do
24     host -l uit.edu.vn "$ns"
25 done

```

```
26
27 echo "/nhcmut:"
28 for ns in "${hcmut[@]}"; do
29     host -l hcmut.edu.vn "$ns"
30 done
31
32 echo "/nhcmiu:"
33 for ns in "${hcmiu[@]}"; do
34     host -l hcmiu.edu.vn "$ns"
35 done
36
37 echo "/nuel:"
38 for ns in "${uel[@]}"; do
39     host -l uel.edu.vn "$ns"
40 done
41
42 echo "/nhcmier:"
43 for ns in "${hcmier[@]}"; do
44     host -l hcmier.edu.vn "$ns"
45 done
46
47 echo "/nvnuhcm:"
48 for ns in "${vnuhcm[@]}"; do
49     host -l vnuhcm.edu.vn "$ns"
50 done
51
```

➔ Kết quả:

```
hcmus:
;; Connection to 115.73.217.121#53(115.73.217.121) for hcmus.edu.vn failed: timed out.
;; Connection to 115.73.217.121#53(115.73.217.121) for hcmus.edu.vn failed: timed out.
;; Connection to 14.161.22.31#53(14.161.22.31) for hcmus.edu.vn failed: timed out.
;; Connection to 14.161.22.31#53(14.161.22.31) for hcmus.edu.vn failed: timed out.
Using domain server:
Name: server.hcmus.edu.vn
Address: 171.244.202.180#53
Aliases:

Host hcmus.edu.vn not found: 5(REFUSED)
; Transfer failed.
/nhcmussh:
Using domain server:
Name: server.vnuhcm.edu.vn
Address: 103.88.121.201#53
Aliases:

Host hcmussh.edu.vn not found: 5(REFUSED)
; Transfer failed.
Using domain server:
Name: vnuserv.vnuhcm.edu.vn
Address: 103.88.121.200#53
Aliases:

Host hcmussh.edu.vn not found: 5(REFUSED)
; Transfer failed.
/nuit:
Using domain server:
Name: nsbak.pavietnam.net
Address: 112.213.89.22#53
Aliases:

Host uit.edu.vn not found: 5(REFUSED)
; Transfer failed.
Using domain server:
Name: ns1.pavietnam.vn hcmier.edu.vn
Address: 112.213.89.3#53
Aliases:

Host uit.edu.vn not found: 5(REFUSED)
; Transfer failed.
```

```
Using domain server:
Name: ns2.pavietnam.vn
Address: 222.255.121.247#53
Aliases:
Host uit.edu.vn not found: 5(REFUSED).VN "sns"
; Transfer failed.
/nhcmut:
Using domain server:
Name: dns3.hcmut.edu.vn
Address: 203.205.32.235#53
Aliases:
Host hcmut.edu.vn not found: 5(REFUSED)
; Transfer failed.
Using domain server:
Name: dns2.hcmut.edu.vn
Address: 221.133.13.115#53
Aliases:
Host hcmut.edu.vn not found: 5(REFUSED)
; Transfer failed.
;; Connection to 203.205.32.236#53(203.205.32.236) for hcmut.edu.vn failed: timed out.
;; Connection to 203.205.32.236#53(203.205.32.236) for hcmut.edu.vn failed: timed out.
Using domain server:
Name: dns1.hcmut.edu.vn
Address: 101.99.31.218#53
Aliases:
Host hcmut.edu.vn not found: 5(REFUSED)
; Transfer failed.
/nhcmiu:
Using domain server:
Name: hcm-server1.vnn.vn
Address: 203.162.4.1#53
Aliases:
Host hcmiu.edu.vn not found: 5(REFUSED)
; Transfer failed.
```



```

Using domain server:
Name: vdc-hn01.vnn.vn
Address: 203.162.0.11#53
Aliases:
Host hcmiu.edu.vn not found: 5(REFUSED)
; Transfer failed.
/nuel:
Using domain server:
Name: ns1.dns.net.vn
Address: 210.211.108.160#53
Aliases:
Host uel.edu.vn not found: 5(REFUSED)
; Transfer failed.
Using domain server:
Name: ns2.dns.net.vn
Address: 103.45.229.100#53
Aliases:
Host uel.edu.vn not found: 5(REFUSED)
; Transfer failed.
/nhcmier:
Using domain server:
Name: server.vnuhcm.edu.vn
Address: 103.88.121.201#53
Aliases:
Host hcmier.edu.vn not found: 5(REFUSED)
; Transfer failed.
Using domain server:
Name: vnuserv.vnuhcm.edu.vn
Address: 103.88.121.200#53
Aliases:
Host hcmier.edu.vn not found: 5(REFUSED)
; Transfer failed.
/nvnuhcm:
Using domain server:
Name: server.vnuhcm.edu.vn
Address: 103.88.121.201#53
Aliases:
Host vnuhcm.edu.vn not found: 5(REFUSED)
; Transfer failed.

```

```

Using domain server:
Name: vnuserv.vnuhcm.edu.vn
Address: 103.88.121.200#53
Aliases:
Host vnuhcm.edu.vn not found: 5(REFUSED)
; Transfer failed.
Using domain server:
Name: ns2.vdc2.vn
Address: 14.225.232.26#53
Aliases:
vnuhcm.edu.vn has address 103.88.121.29
vnuhcm.edu.vn name server vnuserv.vnuhcm.edu.vn.
vnuhcm.edu.vn name server server.vnuhcm.edu.vn.
www.4s.vnuhcm.edu.vn has address 118.69.204.199
aaa.vnuhcm.edu.vn has address 103.88.123.21
aaa1.vnuhcm.edu.vn has address 103.88.123.22
aad.vnuhcm.edu.vn has address 203.162.44.60
ab.vnuhcm.edu.vn has address 203.162.147.252
aun.vnuhcm.edu.vn has address 203.162.147.168
baixektx.vnuhcm.edu.vn has address 123.30.236.140
baocaoaad.vnuhcm.edu.vn has address 203.162.44.60
mssql.baocaoaad.vnuhcm.edu.vn has address 203.162.44.60
betaaad.vnuhcm.edu.vn has address 222.255.69.252
cdio2015.vnuhcm.edu.vn has address 221.133.13.127
cea.vnuhcm.edu.vn has address 103.88.123.7
csgd.cea.vnuhcm.edu.vn has address 103.88.123.7
database.cea.vnuhcm.edu.vn has address 103.88.123.7
dkht.cea.vnuhcm.edu.vn has address 103.88.123.7
cete.vnuhcm.edu.vn has address 103.88.123.2
chrd.vnuhcm.edu.vn has address 203.162.147.149
club.vnuhcm.edu.vn has address 203.162.147.185
www.cntttt.vnuhcm.edu.vn has address 203.162.44.72
congdoan.vnuhcm.edu.vn has address 118.69.123.142
cpmu-demo.vnuhcm.edu.vn has address 103.88.121.59
cpmu-demo1.vnuhcm.edu.vn has address 112.78.11.146
cps.vnuhcm.edu.vn has address 112.78.11.146
ct.vnuhcm.edu.vn has address 203.162.147.252
data.vnuhcm.edu.vn has address 203.162.147.185
dataonline.vnuhcm.edu.vn has address 203.162.44.60
demo.vnuhcm.edu.vn has address 103.88.121.29
demo-cloud.vnuhcm.edu.vn has address 103.88.121.64
demo-khcn.vnuhcm.edu.vn has address 203.162.147.185
demo-lms.vnuhcm.edu.vn has address 103.88.121.142

```

```

demo-portal.vnuhcm.edu.vn has address 203.128.241.215
demo-portal-admin.vnuhcm.edu.vn has address 203.128.241.215
demo-portal-static.vnuhcm.edu.vn has address 203.128.241.21
demo1.vnuhcm.edu.vn has address 203.162.147.185
demotuyensinh.vnuhcm.edu.vn has address 203.162.147.186
doancoquan.vnuhcm.edu.vn has address 203.162.147.186
doancoquan.vnuhcm.edu.vn has address 103.74.123.10
doantn.vnuhcm.edu.vn has address 203.162.44.83
email-reply.vnuhcm.edu.vn has address 103.88.121.53
gddhhoinhapquocte.vnuhcm.edu.vn has address 123.30.191.189
greeting-card.vnuhcm.edu.vn has address 203.162.147.185
hoidong.vnuhcm.edu.vn has address 203.162.147.185
hoithaocokhi.vnuhcm.edu.vn has address 165.22.97.200
hoithaogiaothong.vnuhcm.edu.vn has address 206.189.35.164
hosting.vnuhcm.edu.vn has address 203.162.147.185
hotrokythuat.vnuhcm.edu.vn has address 112.78.11.146
idm.vnuhcm.edu.vn has address 103.88.123.51
it-support.vnuhcm.edu.vn has address 112.78.11.146
jobs.vnuhcm.edu.vn has address 103.88.123.54
khaosat.vnuhcm.edu.vn has address 203.162.147.185
khn.vnuhcm.edu.vn has address 203.162.147.185
quanly.khn.vnuhcm.edu.vn has address 118.69.123.142
khcn2018.vnuhcm.edu.vn has address 103.88.121.35
khoanhkhacdothidaihoc.vnuhcm.edu.vn has address 123.30.78.232
kituxa.vnuhcm.edu.vn has address 45.117.77.102
ksknsvt.vnuhcm.edu.vn has address 203.162.44.60
ktx.vnuhcm.edu.vn has address 45.117.77.103
mail.ktx.vnuhcm.edu.vn has address 203.162.44.60
ktxdhqg.vnuhcm.edu.vn has address 45.117.77.102
ktxdhqghcm.vnuhcm.edu.vn has address 123.30.236.140
lichtuan.vnuhcm.edu.vn has address 203.162.147.195
live.vnuhcm.edu.vn has address 42.116.11.16
manage-01.vnuhcm.edu.vn has address 103.88.123.64
manage-02.vnuhcm.edu.vn has address 103.88.121.41
meeting.vnuhcm.edu.vn has address 203.162.147.247
noc.vnuhcm.edu.vn has address 112.78.10.40
ns.vnuhcm.edu.vn has address 14.225.232.25
ns1.vnuhcm.edu.vn has address 14.225.232.25
ns2.vnuhcm.edu.vn has address 14.225.232.25
ntb.vnuhcm.edu.vn has address 103.88.88.88
phapluat.vnuhcm.edu.vn has address 74.86.148.43
portal-st.vnuhcm.edu.vn has address 103.88.121.38
qlcb.vnuhcm.edu.vn has address 118.69.123.137
qlda-vp.vnuhcm.edu.vn has address 103.88.121.138
qlda-xd.vnuhcm.edu.vn has address 103.88.121.137
qtmvp.vnuhcm.edu.vn has address 203.163.1.150
quanlydetai.vnuhcm.edu.vn has address 115.78.164.32
rankingdata.vnuhcm.edu.vn has address 103.88.121.33
rk.vnuhcm.edu.vn has address 103.88.121.33
rkd.vnuhcm.edu.vn has address 103.88.121.33
rm.vnuhcm.edu.vn has address 103.88.121.37
rnm.vnuhcm.edu.vn has address 103.88.121.37
server.vnuhcm.edu.vn has address 103.88.121.201
server.vnuhcm.edu.vn has address 14.225.232.25
server3.vnuhcm.edu.vn has address 203.162.147.149
sm-vnu.vnuhcm.edu.vn has address 203.162.44.47
static.vnuhcm.edu.vn has address 103.88.121.29
svktx.vnuhcm.edu.vn has address 45.117.77.102
tapchikhoahoc.vnuhcm.edu.vn has address 203.162.147.185
tchc.vnuhcm.edu.vn has address 203.162.147.241
test.vnuhcm.edu.vn has address 203.162.147.186
testbed.vnuhcm.edu.vn has address 203.162.44.55
testing.vnuhcm.edu.vn has address 203.162.147.179
testweb.vnuhcm.edu.vn has address 123.30.78.233
thinangluc.vnuhcm.edu.vn has address 118.69.123.136
thinangluc.vnuhcm.edu.vn has address 45.122.249.72
thinangluc-test.vnuhcm.edu.vn has address 221.133.13.124
thumoi.vnuhcm.edu.vn has address 125.253.116.180
thuongnien.vnuhcm.edu.vn has address 203.162.147.252
tspl.vnuhcm.edu.vn has address 203.162.44.60
ttgdqp.vnuhcm.edu.vn has address 222.255.69.250
ttqlptkdt.vnuhcm.edu.vn has address 203.162.44.60
ttqlptkdt-beta.vnuhcm.edu.vn has address 203.162.44.60
tttdtt.vnuhcm.edu.vn has address 103.88.123.130
tuoitre.vnuhcm.edu.vn has address 210.211.118.168
tuvantuyensinh.vnuhcm.edu.vn has address 203.162.147.185
dangky.tuyensinh.vnuhcm.edu.vn has address 203.162.147.196
vc.vnuhcm.edu.vn has address 171.244.28.100
vnu-f.vnuhcm.edu.vn has address 103.88.121.141
www.vnu-f.vnuhcm.edu.vn has address 103.88.121.141
vnu-f2.vnuhcm.edu.vn has address 103.88.123.5
vnu20.vnuhcm.edu.vn has address 203.162.147.185
vnuc.vnuhcm.edu.vn has address 112.78.11.146
vnuserv.vnuhcm.edu.vn has address 103.88.121.200
vnuserv.vnuhcm.edu.vn has address 14.225.232.25
voice.vnuhcm.edu.vn has address 203.162.147.187
wifi.vnuhcm.edu.vn has address 10.238.239.1
www.vnuhcm.edu.vn has address 103.88.121.29
Using domain server:
Name: ns1.vdc2.vn
Address: 14.225.232.25#53
Aliases:
vnuhcm.edu.vn host not found: 5(REFUSED)
Host vnuhcm.edu.vn not found: 5(REFUSED)
; Transfer failed.

```

26.

-t std (Standard Enumeration): kiểm tra các bản ghi dns cơ bản cho một tên miền.

-t rv1 (Reverse IP Enumeration): tìm kiếm subdomains bằng cách kiểm tra tên miền ngược.

- t tld (Top Level Domain Enumeration): liệt kê tất cả các tên miền cấp cao nhất đã biết.
- t zon (Zone Transfer Enumeration): thử thực hiện zone transfer trên máy chủ DNS mục tiêu.
- t goo (Google Enumeration): tìm kiếm thông tin về tên miền thông qua Google.
- t fwd (Forward Lookup Enumeration): kiểm tra bản ghi DNS dựa trên IP.
- t sec (DNSSEC Enumeration): tìm kiếm thông tin về DNSSEC.
- t axfr (Subdomain Enumeration with Wordlist): kiểm tra các subdomains bằng cách sử dụng wordlist.
- t brt (Brute Force Subdomains Enumeration): tấn công brute force trên subdomains.

27.

dnsrecon -d megacorpone.com -t std

```
(kali㉿kali)-[~/Desktop]
$ dnsrecon -d megacorpone.com -t std

[*] std: Performing General Enumeration against: megacorpone.com...
[-] DNSSEC is not configured for megacorpone.com
[*] SOA ns1.megacorpone.com 51.79.37.18
[*] NS ns1.megacorpone.com 51.79.37.18
[*] Bind Version for 51.79.37.18 "9.11.5-P4-5.1+deb10u2-Debian"
[*] NS ns3.megacorpone.com 66.70.207.180
[*] Bind Version for 66.70.207.180 "9.11.5-P4-5.1+deb10u2-Debian"
[*] NS ns2.megacorpone.com 51.222.39.63
[*] Bind Version for 51.222.39.63 "9.11.5-P4-5.1+deb10u2-Debian"
[*] MX mail.megacorpone.com 51.222.169.212
[*] MX spool.mail.gandi.net 217.70.178.1
[*] MX mail2.megacorpone.com 51.222.169.213
[*] MX fb.mail.gandi.net 217.70.178.215
[*] MX fb.mail.gandi.net 217.70.178.217
[*] MX fb.mail.gandi.net 217.70.178.216
[*] MX spool.mail.gandi.net 2001:4b98:e00::1
[*] MX fb.mail.gandi.net 2001:4b98:dc4:8::216
[*] MX fb.mail.gandi.net 2001:4b98:dc4:8::215
[*] MX fb.mail.gandi.net 2001:4b98:dc4:8::217
[*] TXT megacorpone.com Try Harder
[*] TXT megacorpone.com google-site-verification=U7B_b0HNeBtY4qYGQZNsEYXfCJ32hMNV3GtC0wWq5pA
[*] Enumerating SRV Records
[+] 0 Records Found
```

dnsrecon -d megacorpone.com -t tld

```
(kali㉿kali)-[~/Desktop]
$ dnsrecon -d megacorpone.com -t tld
[*] tld: Performing TLD Brute force Enumeration against megacorpone.com...
[*] The operation could take up to: 00:01:35
[+] A megacorpone.org 3.33.130.190
[+] A megacorpone.org 15.197.148.33
[+] A megacorpone.net 38.100.193.76
[+] A megacorpone.online 54.152.8.65
[+] A megacorpone.ph 45.79.222.138
[+] A megacorpone.vg 88.198.29.97
[+] A megacorpone.ws 64.70.19.203
[+] A megacorpone.aq.biz 13.248.169.48
[+] A megacorpone.aq.biz 76.223.54.146
[+] A stormbird-694598537.us-west-1.elb.amazonaws.com 54.215.0.24
[+] A stormbird-694598537.us-west-1.elb.amazonaws.com 52.52.203.198
[+] A megacorpone.bb.info 170.178.183.18
[+] A megacorpone.bo.org 64.190.63.111
[+] 13 Records Found
```

28.

- Độ dễ sử dụng:

+ DNSEnum: thiết kế đơn giản và dễ sử dụng, giao diện trực quan giúp người dùng dễ dàng kiểm tra và thu thập thông tin DNS.

+ DNSRecon: giao diện dòng lệnh và cung cấp nhiều tùy chọn mạnh mẽ, hữu ích với người dùng có kinh nghiệm, phức tạp cho người dùng mới.

- Kết quả chính xác:

+ DNSEnum: kiểm tra cơ bản với các tùy chọn mặc định nhưng có thể không cung cấp kết quả chính xác.

+ DNSRecon: cung cấp nhiều tùy chọn tùy chỉnh giúp kiểm tra chi tiết hơn, nếu cấu hình đúng cách nó có thể cung cấp kết quả chính xác hơn.

- Hiển thị kết quả:

+ DNSEnum: dưới dạng danh sách tên miền và subdomains trong giao diện dòng lệnh.

+ DNSRecon: nhiều định dạng đầu ra, bao gồm JSON, XML, CSV giúp dễ lưu trữ và phân tích kết quả.

➔ DNSEnum thích hợp cho người dùng mới và kiểm tra nhanh, DNSRecon thích hợp cho người muốn kiểm tra chi tiết hơn và cần nhiều tùy chọn tùy chỉnh.

29.

Kiểm tra địa chỉ IP của máy ảo megacorpone:


```

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:fa:dd:2a
          inet addr:192.168.6.135  Bcast:192.168.6.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fefa:dd2a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:82 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7020 (6.8 KB)  TX bytes:7494 (7.3 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:122 errors:0 dropped:0 overruns:0 frame:0
          TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:33885 (33.0 KB)  TX bytes:33885 (33.0 KB)

```

Thực hiện quét port

```

(kali@kali)-[~]
$ sudo nmap -sS 192.168.6.135
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 04:50 EDT
Nmap scan report for 192.168.6.135
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds

```

Bắt Wireshark:

5	0.132021319	192.168.6.132	192.168.6.135	TCP	58 61592 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	0.132205418	192.168.6.132	192.168.6.135	TCP	58 61592 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	0.132351319	192.168.6.132	192.168.6.135	TCP	58 61592 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	0.132557018	192.168.6.135	192.168.6.132	TCP	60 110 → 61592 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
9	0.132567218	192.168.6.135	192.168.6.132	TCP	60 135 → 61592 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10	0.132679118	192.168.6.135	192.168.6.132	TCP	60 1025 → 61592 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	0.132727118	192.168.6.132	192.168.6.135	TCP	58 61592 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	0.132851118	192.168.6.132	192.168.6.135	TCP	58 61592 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	0.132955818	192.168.6.132	192.168.6.135	TCP	58 61592 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	0.133110419	192.168.6.135	192.168.6.132	TCP	60 554 → 61592 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	0.133180718	192.168.6.132	192.168.6.135	TCP	58 61592 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	0.133190119	192.168.6.135	192.168.6.132	TCP	60 111 → 61592 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
17	0.133343219	192.168.6.132	192.168.6.135	TCP	54 61592 → 111 [RST] Seq=1 Win=0 Len=0

Port 1:

No.	Time	Source	Destination	Protocol	Length	Info
767	0.191294027	192.168.6.132	192.168.6.135	TCP	58	61592 → 1 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
786	0.191967227	192.168.6.135	192.168.6.132	TCP	60	1 → 61592 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Máy ta (192.168.6.132) gửi gói tin SYN đến port 1 của máy mục tiêu (192.168.6.132)

- ➔ Nmap gửi gói tin TCP có cờ SYN đến máy mục tiêu trên port 1. Gói tin SYN được sử dụng để bắt đầu quá trình thiết lập một kết nối TCP, thể hiện ý định thiết lập kết nối với máy chủ.

Máy mục tiêu gửi gói tin RST đến máy ta.

- ➔ Nếu cổng đang đóng hoặc máy chủ không thể kết nối, máy mục tiêu sẽ gửi gói tin RST (Reset), thể hiện rằng kết nối không thể thiết lập và cổng đang đóng.

Port 21:

No.	Time	Source	Destination	Protocol	Length	Info
63	0.137184219	192.168.6.132	192.168.6.135	TCP	58	61592 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
66	0.137450919	192.168.6.135	192.168.6.132	TCP	60	21 → 61592 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
67	0.137464119	192.168.6.132	192.168.6.135	TCP	54	61592 → 21 [RST] Seq=1 Win=0 Len=0

Máy ta gửi gói tin SYN đến port 21 máy mục tiêu.

Máy mục tiêu gửi gói tin SYN-ACK đến máy ta.

- ➔ Cổng được quét đang mở, máy mục tiêu gửi gói tin trả lời lại. Thể hiện rằng máy chủ đã chấp nhận kết nối và đang chuẩn bị thiết lập một kết nối TCP.

Máy ta gửi gói tin RST đến máy mục tiêu.

- ➔ Kết thúc kết nối.

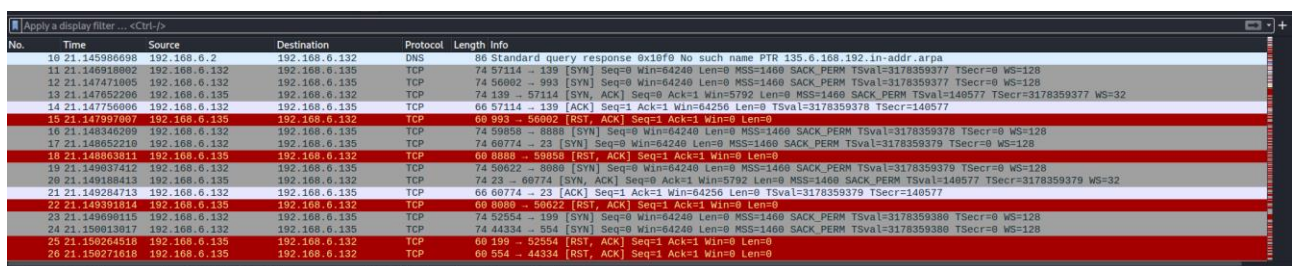
30.

Quét port:


```
(kali㉿kali)-[~]
$ sudo nmap -sT 192.168.6.135
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 05:12 EDT
Nmap scan report for 192.168.6.135
Host is up (0.0026s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

Wireshark:



Port 25:

No.	Time	Source	Destination	Protocol	Length	Info
66	21.157538152	192.168.6.132	192.168.6.135	TCP	74	56584 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3178359387 TSecr=0 WS=128
68	21.157977954	192.168.6.135	192.168.6.132	TCP	74	25 → 56584 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=140578 TSecr=3178359387 WS=32
69	21.158098454	192.168.6.132	192.168.6.135	TCP	66	56584 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3178359388 TSecr=140578
91	21.162186173	192.168.6.132	192.168.6.135	TCP	66	56584 → 25 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 TSval=3178359392 TSecr=140578

Máy ta gửi đến máy mục tiêu gói tin SYN đến port 25.

Máy mục tiêu gửi lại gói tin SYN, ACK -> port đang mở và máy chủ chấp nhận kết nối.

Máy ta gửi gói tin ACK đến máy mục tiêu -> xác nhận máy ta đã nhận gói tin SYN, ACK và sẵn sàng thiết lập kết nối, quá trình này hoàn thành việc kết nối TCP 2 chiều.

Máy ta gửi gói tin RST, ACK cho máy mục tiêu -> máy chúng ta muốn kết thúc kết nối TCP, chờ ACK xác nhận việc gửi gói tin RST.

31.

- Số lượng gói tin được gửi và nhận:

+ SYN Scan: Nmap chỉ gửi gói tin SYN tới máy mục tiêu trên các cổng mục tiêu. Không thiết lập kết nối TCP hoàn chỉnh, chỉ nhận gói tin SYN-ACK hoặc RST từ máy mục tiêu để xác định trạng thái của port.

+ TCP Connect Scan: Nmap gửi gói tin SYN để mở kết nối, sau đó gửi gói tin ACK để hoàn thành kết nối TCP, và cuối cùng đóng kết nối bằng cách gửi gói tin RST. Số lượng gói tin gửi và nhận trong TCP Connect Scan nhiều hơn so với SYN Scan vì nó thiết lập và đóng kết nối TCP hoàn chỉnh.

- Thời gian quét:

+ SYN Scan: nhanh hơn.

+ TCP Connect Scan: mất nhiều thời gian hơn vì thiết lập và đóng kết nối TCP hoàn chỉnh cho mỗi port.

- Kết quả hiển thị: hiển thị tình trạng cổng mục tiêu tương tự nhau.

32.

Đoạn code kiểm tra bằng Python:

```
1 import os
2
3 IP = input("Host IP address: ")
4 print("Starting... ")
5 dot = IP.rfind(".")
6 IP = IP[0:dot + 1]
7
8 for i in range(1, 255):
9     host = IP + str(i)
10    reponse = os.system("ping -c 1 -w 1 " + host + " >/dev/null")
11
12    if reponse == 0:
13        print(host + " is up")
14 |
```

Kết quả chạy:

```
(kali@kali)-[~/Desktop/NetworkSecurity]
$ python scan.py
Host IP address: 192.168.6.2
Starting ...
192.168.6.2 is up
192.168.6.132 is up
192.168.6.135 is up
[
python3 --help=416 --UP, BROADCAST, RUNNING, MULTICA
```

33.

Quét hosts:

```
(kali@kali)-[~]
$ nmap -sn 192.168.6.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 05:50 EDT
Nmap scan report for 192.168.6.2
Host is up (0.0017s latency).
Nmap scan report for 192.168.6.132
Host is up (0.00030s latency).
Nmap scan report for 192.168.6.135
Host is up (0.0037s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.45 seconds
```

Wireshark:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.6.132	192.168.6.1	TCP	74	35328 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3705996413 TSecr=0 WS=128
2	0.000227501	192.168.6.132	192.168.6.2	TCP	74	60120 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=336198091 TSecr=0 WS=128
3	0.000438808	192.168.6.2	192.168.6.132	TCP	60	80 → 60120 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
4	0.000451408	VMware_76:ce:35	Broadcast	ARP	42	Who has 192.168.6.3? Tell 192.168.6.132
5	0.000617708	VMware_76:ce:35	Broadcast	ARP	42	Who has 192.168.6.4? Tell 192.168.6.132
6	0.000842908	VMware_76:ce:35	Broadcast	ARP	42	Who has 192.168.6.5? Tell 192.168.6.132
7	0.001035399	VMware_76:ce:35	Broadcast	ARP	42	Who has 192.168.6.6? Tell 192.168.6.132
8	0.001189699	VMware_76:ce:35	Broadcast	ARP	42	Who has 192.168.6.7? Tell 192.168.6.132
9	0.001360199	VMware_76:ce:35	Broadcast	ARP	42	Who has 192.168.6.8? Tell 192.168.6.132
10	0.001508299	VMware_76:ce:35	Broadcast	ARP	42	Who has 192.168.6.9? Tell 192.168.6.132
11	0.001655099	VMware_76:ce:35	Broadcast	ARP	42	Who has 192.168.6.10? Tell 192.168.6.132
12	0.002163198	VMware_76:ce:35	Broadcast	ARP	42	Who has 192.168.6.13? Tell 192.168.6.132
13	0.002343797	VMware_76:ce:35	Broadcast	ARP	42	Who has 192.168.6.14? Tell 192.168.6.132
14	0.100152561	VMware_76:ce:35	Broadcast	ARP	42	Who has 192.168.6.19? Tell 192.168.6.132
15	0.100543161	VMware_76:ce:35	Broadcast	ARP	42	Who has 192.168.6.22? Tell 192.168.6.132
16	0.101125168	VMware_76:ce:35	Broadcast	ARP	42	Who has 192.168.6.25? Tell 192.168.6.132
17	0.101351159	VMware_76:ce:35	Broadcast	ARP	42	Who has 192.168.6.26? Tell 192.168.6.132

Những host đang hoạt động sẽ gửi gói tin trả lời:

No.	Time	Source	Destination	Protocol	Length	Info
515	2.003676841	192.168.6.132	192.168.6.135	TCP	66	33848 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3180612681 TSecr=365894
516	2.003909348	192.168.6.132	192.168.6.135	TCP	66	33848 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3180612681 TSecr=365894
513	2.003024641	192.168.6.132	192.168.6.135	TCP	74	33848 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3180612680 TSecr=0 WS=128
1	0.000000000	192.168.6.132	192.168.6.1	TCP	74	35328 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3705996413 TSecr=0 WS=128
269	1.101508675	192.168.6.132	192.168.6.1	TCP	74	40414 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3705997514 TSecr=0 WS=128
270	1.104196771	192.168.6.132	192.168.6.1	TCP	74	41158 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3705997517 TSecr=0 WS=128
299	1.205390231	192.168.6.132	192.168.6.1	TCP	74	41162 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3705997618 TSecr=0 WS=128
451	1.708563741	192.168.6.132	192.168.6.254	TCP	74	41238 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1738514474 TSecr=0 WS=128
141	0.511506487	192.168.6.132	192.168.6.254	TCP	74	44396 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1738513277 TSecr=0 WS=128
517	2.015633825	192.168.6.132	192.168.6.254	TCP	74	44600 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1738514782 TSecr=0 WS=128
528	2.115988788	192.168.6.132	192.168.6.254	TCP	74	44604 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1738514882 TSecr=0 WS=128
60	0.404726237	192.168.6.132	192.168.6.135	TCP	66	50778 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3180611082 TSecr=365734
82	0.408251732	192.168.6.132	192.168.6.135	TCP	66	50778 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3180611085 TSecr=365734
55	0.404130039	192.168.6.132	192.168.6.135	TCP	74	50778 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3180611081 TSecr=0 WS=128
2	0.000227501	192.168.6.132	192.168.6.2	TCP	74	60120 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=336198091 TSecr=0 WS=128
514	2.003624041	192.168.6.135	192.168.6.132	TCP	74	80 → 33848 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=365894 TSecr=3180612680 WS=32
59	0.404673037	192.168.6.135	192.168.6.132	TCP	74	80 → 50778 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=365734 TSecr=3180611081 WS=32

34.

```

kali@kali:~$ sudo nmap -sV -sT -A 192.168.6.135
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 05:59 EDT
Nmap scan report for 192.168.6.135
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
|_ ftp-syst:
|_ STAT:
|_ FTP server status:
|_   Connected to 192.168.6.132
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit
|_   Session timeout in seconds is 300
|_   Control connection is plain text
|_   Data connections will be plain text
|_   vsFTPD 2.3.4 - secure, fast, stable
|_ End of status
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ ssh-hostkey:
|_   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)  ed (592 bits) on interface eth0, id 0
|_   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)  Dst: VMware:fa:dd:2a (00:0c:29:fa:dd:2a)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp          Postfix smtpd
|_ sslv2:
|_   SSLv2 supported
|_   ciphers:
|_     SSL2_RC4_128_EXPORT40_WITH_MD5
|_     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_     SSL2_RC4_128_WITH_MD5
|_     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_     SSL2_DES_64_CBC_WITH_MD5
|_     SSL2_RC2_128_CBC_WITH_MD5
|_ ssl-date: 2023-10-24T09:59:38+00:00; +3s from scanner time.
|_ ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no
such thing outside US/countryName=XX
|_ Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
|_ smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES
, 8BITMIME, DSN
53/tcp    open  domain        ISC BIND 9.4.2
|_ dns-nsid:
|_   bind.version: 9.4.2

```



```

80/tcp open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp open  rpcbind    2 (RPC #100000)
|_rpcinfo:
|_  program version  port/proto  service
|_  100000 2 111/tcp rpcbind
|_  100000 2 111/udp rpcbind
|_  100003 2,3,4 2049/tcp nfs
|_  100003 2,3,4 2049/udp nfs
|_  100005 1,2,3 36391/udp mountd
|_  100005 1,2,3 60779/tcp mountd
|_  100021 1,3,4 34557/udp nlockmgr
|_  100021 1,3,4 52459/tcp nlockmgr
|_  100024 1 47327/tcp status
|_  100024 1 59168/udp status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  smb Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec netkit-rsh rexecd
513/tcp open  login
514/tcp open  tcpwrapped
1099/tcp open  java-rmi GNU Classpath grmiregistry
1524/tcp open  bindshell Metasploitable root shell
2049/tcp open  nfs 2-4 (RPC #100003)
2121/tcp open  ftp ProFTPD 1.3.1
3306/tcp open  mysql MySQL 5.0.51a-3ubuntu5
|_mysql-info:
|_  Protocol: 10
|_  Version: 5.0.51a-3ubuntu5
|_  Thread ID: 10
|_  Capabilities flags: 43564
|_  Some Capabilities: Support41Auth, LongColumnFlag, SupportsCompression, SupportsTransactions, ConnectWithDatabase, SwitchToSSLAfterHandshake, Speaks41ProtocolNew
|_  Status: Autocommit
|_  Salt: 1srwU!8gb7)gLyQg3
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-10-24T09:59:38+00:00; +3s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
5900/tcp open  vnc VNC (protocol 3.3)
|_vnc-info:
|_  Protocol version: 3.3
|_  Security types:
|_  VNC Authentication (2)
6000/tcp open  X11 (access denied)

```

```

6667/tcp open  irc UnrealIRCd
|_irc-info:
|_  users: 1
|_  servers: 1
|_  lusers: 1
|_  lservers: 0
|_  server: irc.Metasploitable.LAN
|_  version: Unreal3.2.8.1. irc.Metasploitable.LAN
|_  uptime: 0 days, 1:14:41
|_  source ident: nmap
|_  source host: 292F178D.E9742FE6.FFFA6D49.IP
|_  error: Closing Link: ptdfqlgty[192.168.6.132] (Quit: ptdfqlgty)
8009/tcp open  ajp13 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1

```

```
Host script results:
|_clock-skew: mean: 1h00m02s, deviation: 2h00m00s, median: 2s
|_smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2023-10-24T05:59:29-04:00
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT      ADDRESS
1   1.06 ms 192.168.6.135

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.10 seconds
```

35.

Dùng NSE “vuln” để kiểm tra các lỗ hổng bảo mật cụ thể trên máy chủ mục tiêu dựa trên các dấu vết và thông tin thu thập trong quá trình quét. Giúp xác định các lỗ hổng và khuyết điểm bảo mật.

```
(kali@kali)-[~]
$ sudo nmap 192.168.6.135 --script=vuln
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 06:07 EDT
```

```
21/tcp open  ftp
|_ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs: BID:48539 CVE:CVE-2011-2523
|   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
|   References:
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.
rb
|   https://www.securityfocus.com/bid/48539
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
22/tcp open  ssh
```



```

http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
http-slowloris-check:
  VULNERABLE:
    Slowloris DOS attack
    State: LIKELY VULNERABLE
    IDs: CVE:CVE-2007-6750
    Slowloris tries to keep many connections to the target web server open and hold
    them open as long as possible. It accomplishes this by opening connections to
    the target web server and sending a partial request. By doing so, it starves
    the http server's resources causing Denial Of Service.

    Disclosure date: 2009-09-17
    References:
      http://ha.ckers.org/slowloris/
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
http-trace: TRACE is enabled
1099/tcp open  rmiregistry
rmi-vuln-classloader:
  VULNERABLE:
    RMI registry default configuration remote code execution vulnerability
    State: VULNERABLE
    Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote co
    de execution.

    References:
      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb

```

NSE “mysql-info” thu thập thông tin về máy chủ MySQL.

```

(kali@kali)-[~]
$ sudo nmap 192.168.6.135 --script=mysql-info
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 06:11 EDT
Nmap scan report for 192.168.6.135
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 121
|   Capabilities flags: 43564
|   Some Capabilities: SupportsTransactions, Speaks41ProtocolNew, SupportsCompression, Support41Auth, LongColumnF
|   lag, SwitchToSSLAfterHandshake, ConnectWithDatabase
|   Status: Autocommit
|   Salt: Zenz;RmMy;W%RMjQ5S"N
5/22/tcp open  postgresql

```

NSE “ftp-anon” kiểm tra máy chủ ftp có cho phép truy cập ẩn danh hay không.

```

(kali@kali)-[~]
$ sudo nmap 192.168.6.135 --script=ftp-anon
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 06:12 EDT
Nmap scan report for 192.168.6.135
21/tcp open  ftp
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp open  ssh

```

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).
Ví dụ: [NT101.K11.ANTT]-Exe01_Group03.
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm bài nộp.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT