



BÁO CÁO THỰC HÀNH

Môn học: An toàn Mạng

Kỳ báo cáo: Session 02

Tên chủ đề: Thu thập thông tin

GVHD: Nghi Hoàng Khoa

Ngày báo cáo: 27/10/2023

Nhóm: 08

1. THÔNG TIN CHUNG:

Lớp: NT140.011.ANTN

STT	Họ và tên	MSSV	Email
1	Nguyễn Vũ Anh Duy	21520211	21520211@gm.uit.edu.vn
2	Lưu Gia Huy	21520916	21520916@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Tất cả các câu (trừ 1->7, 23, 24, 30 đã làm trên lớp)	100%

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

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

BÁO CÁO CHI TIẾT

Câu 8: Bạn có thể tìm kiếm thêm các nhân viên khác của MegaCorp One mà không được liệt kê trên trang web www.megacorpone.com?

Trả lời:

→ Ta sử dụng thêm “intext:name” → Ta sẽ thấy thêm thông tin liên hệ, một số trang web đăng hình ảnh nhân viên.

site:www.megacorpone.com intext:name

Tất cả Hình ảnh Video Mua sắm Sách Thêm Công cụ

Khoảng 20 kết quả (0,27 giây)

[megacorpone.com](https://www.megacorpone.com/contact)
https://www.megacorpone.com › contact

Contact Us - MegaCorp One

Name: Joe Sheer. Title: CEO Email: joe@megacorpone.com. Name: Mike Carlow. Title: VP Of Legal Email: mcarlow@megacorpone.com. Name: Alan Grofield.

Hình ảnh cho site:www.megacorpone.com intext:name

Phản hồi

Xem tất cả →

[megacorpone.com](http://www.megacorpone.com/assets)
http://www.megacorpone.com › assets

Index of /assets/img/team

Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [IMG], james.png, 2016-08-21 11:21, 2.6M. [IMG], joe.jpg, 2016-08-21 11:21 ...

Ảnh kết quả tìm kiếm.

Câu 9: Liệt kê một vài từ khóa thường gặp trên Google và cho ví dụ? (Yêu cầu: ít nhất 5 từ khóa)

Trả lời:

+ “site”: chỉ thực hiện tìm kiếm trên một tên miền nhất định.

Vd: site:www.megacorpone.com

+ “filetype”: để chỉ hiển thị các kết quả có phần mở rộng của tập tin theo chỉ định.

Vd: site:www.megacorpone.com filetype:html

+ “intitle”: trả về các trang web mà tiêu đề của chúng chứa chuỗi nào đó.

Vd: intitle:“Unibox Administration”

+ “intext:name”: tìm các trang trên trang web nào đó mà có từ "name" xuất hiện trong văn bản hoặc bên trong trang.

Vd: site:www.megacorpone.com intext:name

+ “inurl”: Google sẽ hiển thị các trang web có trong URL của họ chứa từ "recipes".

Vd: inurl:recipes

Câu 10: Thực hiện tìm kiếm các tài liệu thú vị của Trường Đại học Công nghệ Thông tin mà được công bố trên Internet mà theo bạn là không nên được công bố?

Trả lời:

→ Thấy được thông tin group mail từ trang daa.uit.edu.vn

2) Group mail của khóa

- Email: sinhvien2022@gm.uit.edu.vn và các email của khóa trên.

- Khi gửi email vào group toàn thể sinh viên của khóa học sẽ nhận được. Group mail này chỉ dùng khi phòng CTSV thông báo hoặc chuyển tiếp thông báo quan trọng của các đơn vị khác đến sinh viên.

Ảnh trích từ lưu ý khi sử dụng email cho sinh viên

→ Thông tin trên không nên đăng công khai vì những thành phần xấu khi nắm được mail sinh viên có thể gửi mail fishing để lừa đảo (nhấp hoặc điền thông tin vào form để nhận thưởng; thực hiện việc khai thác thông tin sinh viên)

Câu 11: Sử dụng Netcraft để xác định máy chủ ứng dụng (application server) đang chạy trên www.megacorpone.com

Trả lời: ta search www.megacorpone.com vào khung search host → Sau đó xem thông tin ở mục Application Servers.

Search Web by Domain

Explore websites visited by users of the Netcraft extensions ↗

Site contains

Example: site contains .netcraft.com

[Search tips](#)

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.calculator.net , www.majorgeeks.com , www.tutorialspoint.com
Debian ↗	No description	www.24presse.com , www.francesoir.fr , www.hhv.de

Kết quả tìm kiếm.

Câu 12: Thực hiện sử dụng module có thể giúp phân giải tên miền ở Hình 20 thành địa chỉ IP tương ứng.

Trả lời: Ta dùng modules “recon/domains-hosts/hackertarget” để phân giải tên miền tìm được: dòng 1 ứng với dòng 20, tương tự (2-19); (3-15); (4-22), kèm theo các domain mới vừa tìm được.

```
[*] 18 total (0 new) hosts found.
[recon-ng][default][hackertarget] > show hosts

+-----+
| rowid | host | ip_address | region | country | latitude | longitude | notes | module |
+-----+
| 1 | support.megacorpone.com | | | | | | | netcraft |
| 2 | intranet.megacorpone.com | | | | | | | netcraft |
| 3 | admin.megacorpone.com | | | | | | | netcraft |
| 4 | www.megacorpone.com | | | | | | | netcraft |
| 5 | fs1.megacorpone.com | 51.222.169.210 | | | | | | hackertarget |
| 6 | ns1.megacorpone.com | 51.79.37.18 | | | | | | hackertarget |
| 7 | mail2.megacorpone.com | 51.222.169.213 | | | | | | hackertarget |
| 8 | ns2.megacorpone.com | 51.222.39.63 | | | | | | hackertarget |
| 9 | www2.megacorpone.com | 149.56.244.87 | | | | | | hackertarget |
| 10 | ns3.megacorpone.com | 66.70.207.180 | | | | | | hackertarget |
| 11 | beta.megacorpone.com | 51.222.169.209 | | | | | | hackertarget |
| 12 | syslog.megacorpone.com | 51.222.169.217 | | | | | | hackertarget |
| 13 | mail.megacorpone.com | 51.222.169.212 | | | | | | hackertarget |
| 14 | siem.megacorpone.com | 51.222.169.215 | | | | | | hackertarget |
| 15 | admin.megacorpone.com | 51.222.169.208 | | | | | | hackertarget |
| 16 | vpn.megacorpone.com | 51.222.169.220 | | | | | | hackertarget |
| 17 | snmp.megacorpone.com | 51.222.169.216 | | | | | | hackertarget |
| 18 | router.megacorpone.com | 51.222.169.214 | | | | | | hackertarget |
| 19 | intranet.megacorpone.com | 51.222.169.211 | | | | | | hackertarget |
| 20 | support.megacorpone.com | 51.222.169.218 | | | | | | hackertarget |
| 21 | test.megacorpone.com | 51.222.169.219 | | | | | | hackertarget |
| 22 | www.megacorpone.com | 149.56.244.87 | | | | | | hackertarget |
+-----+
```

Ảnh kết quả.

Câu 13: Sử dụng một số module khác có trong recon-*ng* để thu thập thông tin về UIT nhiều nhất có thể

Trả lời: vẫn sử dụng modules “recon/domains-hosts/hackertarget” nhưng đổi SOURCE từ “megacorpone.com” thành “uit.edu.vn”.

```
[recon-ng][default][hackertarget] > options set SOURCE uit.edu.vn
SOURCE => uit.edu.vn
[recon-ng][default][hackertarget] > run

UIT.EDU.VN
_____
[*] Country: None
[*] Host: mx1.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: mapr2022.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: a084742fa316491c8c78564efcbce9e0-68f6236f-vm-80.vlab2.uit.edu.vn
[*] Ip_Address: 45.122.249.76
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: host2.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: mx2.uit.edu.vn
```

Ảnh lệnh và kết quả.

→ Ta thu được 104 subdomains từ câu lệnh trên.

SUMMARY					
[*] 104 total (104 new) hosts found.					
[recon-ng][default][hackertarget] > show hosts					
System					
rowid	longitude	notes	module	host	ip_address
					region
					country
					latitude
1		support.megacorpone.com	netcraft		
2		intranet.megacorpone.com	netcraft		
3		admin.megacorpone.com	netcraft		
4		www.megacorpone.com	netcraft		
5		fs1.megacorpone.com	hackertarget		51.222.169.210
6		ns1.megacorpone.com	hackertarget		51.79.37.18
7		mail2.megacorpone.com	hackertarget		51.222.169.213
8		ns2.megacorpone.com	hackertarget		51.222.39.63
9		www2.megacorpone.com	hackertarget		149.56.244.87
10		ns3.megacorpone.com	hackertarget		66.70.207.180
11		beta.megacorpone.com	hackertarget		51.222.169.209
12		syslog.megacorpone.com	hackertarget		51.222.169.217
13		mail.megacorpone.com	hackertarget		51.222.169.212
14		siem.megacorpone.com			51.222.169.215

Ảnh kết quả (do quá dài nên chụp tượng trưng đến dòng 14).

Câu 14: Sử dụng 1 trong 2 công cụ Gitrob hoặc Gitleaks để tìm kiếm các thông tin nhạy cảm bị rò rỉ đối với các trường đại học thành viên trong ĐHQG

Trả lời:

→ Ta git clone code của thầy Vũ Tuấn Hải tại UIT → dùng gitleaks để detect và xuất ra file báo cáo (report.json).

```
(kali㉿kali)-[~/Downloads]
└─$ git clone https://github.com/vutuanhai237/FrontendStudyingBoard.git
Cloning into 'FrontendStudyingBoard'...
remote: Enumerating objects: 5085, done.
remote: Counting objects: 100% (73/73), done.
remote: Compressing objects: 100% (65/65), done.
remote: Total 5085 (delta 51), reused 8 (delta 8), pack-reused 5012
Receiving objects: 100% (5085/5085), 6.68 MiB | 261.00 KiB/s, done.
Resolving deltas: 100% (3340/3340), done.

(kali㉿kali)-[~/Downloads]
└─$ gitleaks detect --source /home/kali/Downloads/FrontendStudyingBoard/ --report-path /home/kali/Downloads/report.json

o
o
o
gitleaks

8:27AM INF 172 commits scanned.
8:27AM INF scan completed in 6.34s
8:27AM WRN leaks found: 1

(kali㉿kali)-[~/Downloads]
```

Ảnh lệnh và kết quả.

→ Ta mở file report.json để check lỗi. → Thấy mô tả của lỗi là “Generic API Key”.

```

1 [
2 {
3   "Description": "Generic API Key",
4   "StartLine": 20,
5   "EndLine": 20,
6   "StartColumn": 26,
7   "EndColumn": 82,
8   "Match": "apikeys\\pgsfnb617zvx79gf1f06sauiik6bg2icroka7q4filexesr\\",
9   "Secret": "pgsfnb617zvx79gf1f06sauiik6bg2icroka7q4filexesr",
10  "File": "src/component/layout/create_post.js",
11  "SymlinkFile": "",
12  "Commit": "1a34ee322de8c67ce0569d661464d17690b14f3a",
13  "Entropy": 4.4900015,
14  "Author": "vutuanhai237",
15  "Email": "a3202025+vutuanhai237@users.noreply.github.com",
16  "Date": "2020-04-28T15:30:13Z",
17  "Message": "Merge branch 'master' of https://github.com/vutuanhai237/Front-end-bht.cnpm.uit.edu.vn\\n\\ncommit aef7a4860c0a6cb6f14a24b78527884a9f872256\\nAuthor: vutuanhai237
\\u003c43202025+vutuanhai237@users.noreply.github.com\\u003e\\rDate: Tue Apr 28 22:28:27 2020 +0700\\n\\nAdd create_post form",
18  "Tags": [],
19  "RuleID": "generic-api-key",
20  "Fingerprint": "1a34ee322de8c67ce0569d661464d17690b14f3a:src/component/layout/create_post.js:generic-api-key:20"
21 }
22 ]
23

```

Ảnh kết quả.

Câu 15: Thực hiện tìm kiếm các lệnh khác trên Shodan mà có thể tiết lộ thêm nhiều thông

tin thú vị về một đối tượng bất kỳ.

Trả lời:

Ta có thể kết hợp thêm các từ khóa làm filter để tìm thêm nhiều thông tin như:

- + City: tìm tại 1 thành phố nào đó.
 - + Country: tìm tại 1 đất nước nào đó.
 - + Geo: tọa độ.
 - + Os: hệ điều hành nào đó.
 - + Net: Ip address.
 - + Hostname: theo hostname.
 - + and 1 filter.
 - or 1 filter.
 - + Before: trước thời gian nào đó.
 - + After: sau thời gian nào đó.
 - + Port: theo port.
- Ta tìm các máy chủ chạy dịch vụ VPN tại Đà Nẵng.

TOTAL RESULTS
376

TOP PORTS

500	369
4500	5
53	1
8090	1

TOP ORGANIZATIONS

Vietnam Posts and Telecommunicati...	228
Viettel Group	91
CMC Telecom Infrastructure Company	23
VietNam Data Communication Company	21
FPT Telecom Company	7
More...	

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access to](#).

203.162.33.98
 static.vnpvt.vn
 VietNam Data Communication Company
 Viet Nam, Da Nang
 vpn
203.205.53.23
 static.cmcti.vn
 CMC Telecom Infrastructure Company
 Viet Nam, Da Nang
 vpn

VPN (IKE)
 Initiator SPI: 6272736768797369
 Responder SPI: 6b7a68366e676aef
 Next Payload: RESERVED
 Version: 2.0
 Exchange Type: DOI Specific Use
 Flags:
 Encryption: False
 Commit: False
 Authentication: False
 Message ID: 00000000
 Length: 36

Initiator SPI: 616b716732663068
 Responder SPI: 317038386a733535
 Next Payload: RESERVED
 Version: 2.0
 Exchange Type: DOI Specific Use
 Flags:

Kết quả tìm kiếm.

Câu 16: So sánh kết quả tìm kiếm trên Shodan so với các search engine khác như Google, Bing...

Trả lời:

Yếu tố so sánh	Shodan	Search Engine khác
Phạm vi tìm kiếm	Chuyên về các thiết bị và hệ thống online	Tất cả trang web
Loại Thông Tin	Thông tin về các thiết bị mạng, máy chủ	Trang web, hình ảnh, văn bản
Mục Tiêu Chính	Bảo mật và tìm kiếm cơ sở hạ tầng mạng	Tìm kiếm toàn diện
Ứng Dụng	Kiểm tra bảo mật hệ thống và thiết bị	Tìm kiếm thông tin chung
Tích Hợp API	Có	Không
Cách Tìm Kiếm	Sử dụng cú pháp đặc biệt và lọc	Tìm kiếm qua trình duyệt
Kết Quả Tìm Kiếm	Đưa ra danh sách thiết bị và thông tin	Hiển thị trang web
Tính Năng Tìm Kiếm Đặc	Tìm kiếm theo port, hệ điều	Tìm kiếm cụ thể, lọc dữ liệu

Biệt	hành, quốc gia	
------	----------------	--

Câu 17: Sử dụng công cụ theHarvester để lấy tìm kiếm các địa chỉ email của UIT

Trả lời:

Ta chỉ định tên miền là uit.edu.vn và nguồn tìm kiếm là baidu. → Tìm được 6 địa chỉ email của UIT.

Ảnh lênh và kết quả.

Câu 18: Sử dụng với nguồn tìm kiếm khác (-b). Theo bạn, kết quả của nguồn nào tốt hơn?

Trả lời:

→ Ta dùng bing làm nguồn tìm kiếm → Kết quả cho ra nhiều email, hosts hơn baidu.

<p>[*] Target: uit.edu.vn</p> <p>Searching 0 results.</p> <p>[*] Searching Bing.</p> <p>[*] No IPs found.</p> <p>[*] Emails found: 37</p> <hr/> <p>01234567@gm.uit.edu.vn bantuyensinh@uit.edu.vn ce@uit.edu.vn chinhnt@uit.edu.vn ctsv@uit.edu.vn cuongvttk@uit.edu.vn hangnm@uit.edu.vn huytl@uit.edu.vn info.https@uit.edu.vn info@uit.edu.vn inseclab@uit.edu.vn khuongnd@uit.edu.vn kietnv@uit.edu.vn nghialh@uit.edu.vn nghianm@uit.edu.vn nhannh@uit.edu.vn nhanpt@uit.edu.vn nhungpt@uit.edu.vn phongctsv@uit.edu.vn phongdaotaodh@uit.edu.vn phongtn@uit.edu.vn phuongltm@uit.edu.vn</p>	<p>ptn.https@uit.edu.vn qlkh@uit.edu.vn qlsdh@uit.edu.vn quangtnn@uit.edu.vn quanlt@uit.edu.vn sangvm@uit.edu.vn sontq@uit.edu.vn thuonght@uit.edu.vn thuvien@uit.edu.vn toannv@uit.edu.vn tungnd@uit.edu.vn tuyensinh@uit.edu.vn vannb@uit.edu.vn vidtn@uit.edu.vn vpdb@uit.edu.vn</p> <hr/> <p>[*] Hosts found: 60</p> <p>acm.uit.edu.vn aiclub.uit.edu.vn auth.uit.edu.vn banglcs.uit.edu.vn binhchon.uit.edu.vn ceday.uit.edu.vn chungthuc.uit.edu.vn cnpm.uit.edu.vn cnsc.uit.edu.vn cntt.uit.edu.vn com.uit.edu.vn cources.uit.edu.vn course.uit.edu.vn courses.uit.edu.vn cs.uit.edu.vn</p>	<p>ctsv.uit.edu.vn cuuv.uit.edu.vn daa.uit.edu.vn dkhp.uit.edu.vn drl.uit.edu.vn dsc.uit.edu.vn ecommerce.uit.edu.vn elearning.uit.edu.vn en.uit.edu.vn fce.uit.edu.vn fit.uit.edu.vn forum.uit.edu.vn gm.uit.edu.vn gmail.uit.edu.vn htt.uit.edu.vn i-english.uit.edu.vn inseclab.uit.edu.vn iot.uit.edu.vn is.uit.edu.vn islab.uit.edu.vn khcn.uit.edu.vn khmt.uit.edu.vn khtc.uit.edu.vn link.uit.edu.vn mail.gm.uit.edu.vn mapr.uit.edu.vn mmlab.uit.edu.vn ms.uit.edu.vn nc.uit.edu.vn nlp.uit.edu.vn oep.uit.edu.vn phongdl.uit.edu.vn portal.uit.edu.vn ptnhttp.uit.edu.vn qhdn.uit.edu.vn qldt.uit.edu.vn</p>
quieter		

Ảnh kết quả.

Câu 19: Thực hiện tìm kiếm các địa chỉ Email của MegaCorp One sử dụng Maltego

Trả lời:

Ta chuột phải vào đối tượng website → chọn “All Transforms” → Chọn **run** trên transform “Mirror: Email addresses found”. → Hiện ra các địa chỉ email mà MegaCorp One sử dụng.



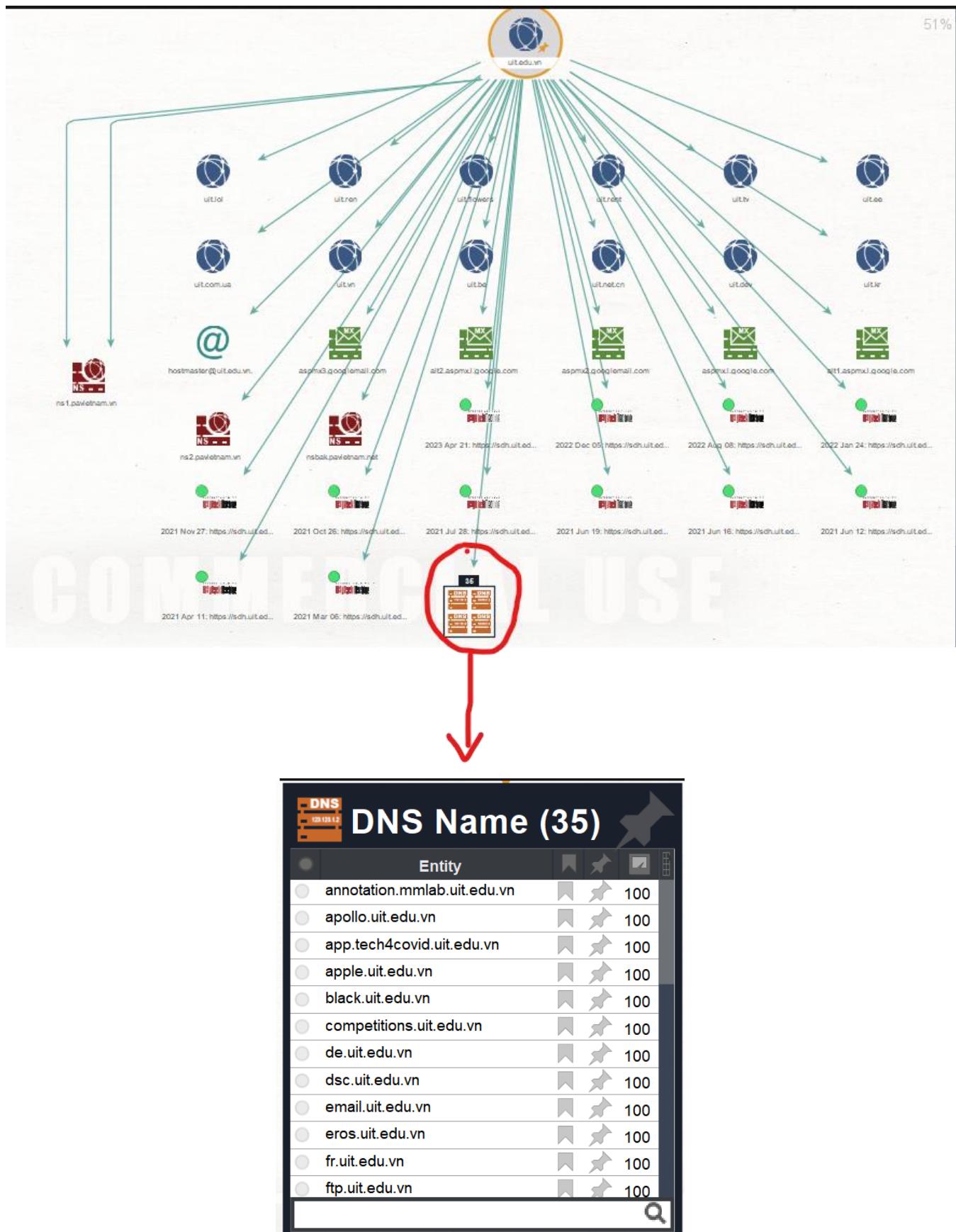
Ảnh kết quả.

Câu 20: Sử dụng công cụ Maltego cho UIT (tên miền: uit.edu.vn) và trả lời các câu hỏi sau:

- a. Các bản ghi DNS.
- b. Các website và địa chỉ IP tương ứng.

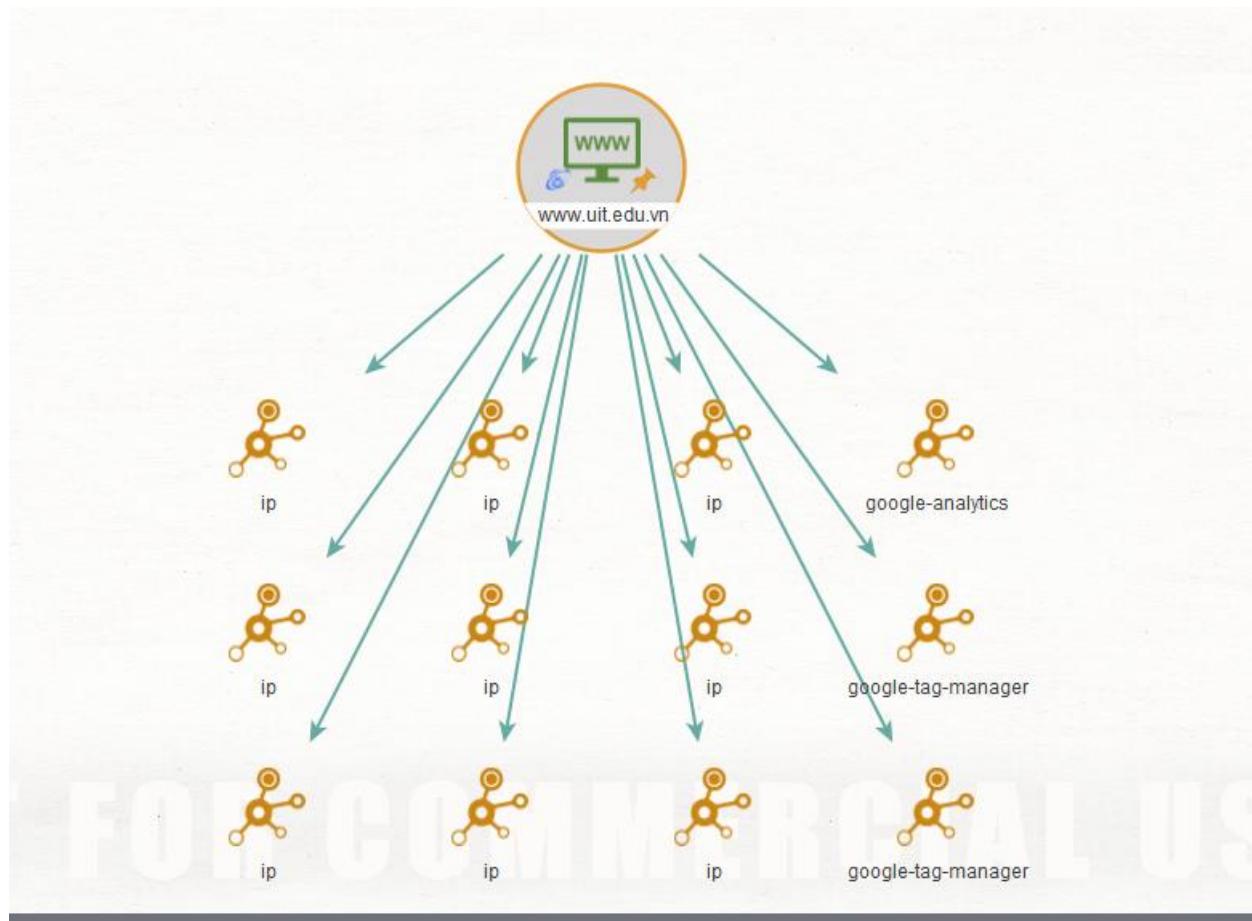
Trả lời:

- a. Ta chuột phải vào domain “uit.edu.vn” → chọn **run** trên “All transforms” → Sau khi chạy xong, sẽ xuất hiện bảng chứa các bản ghi DNS.



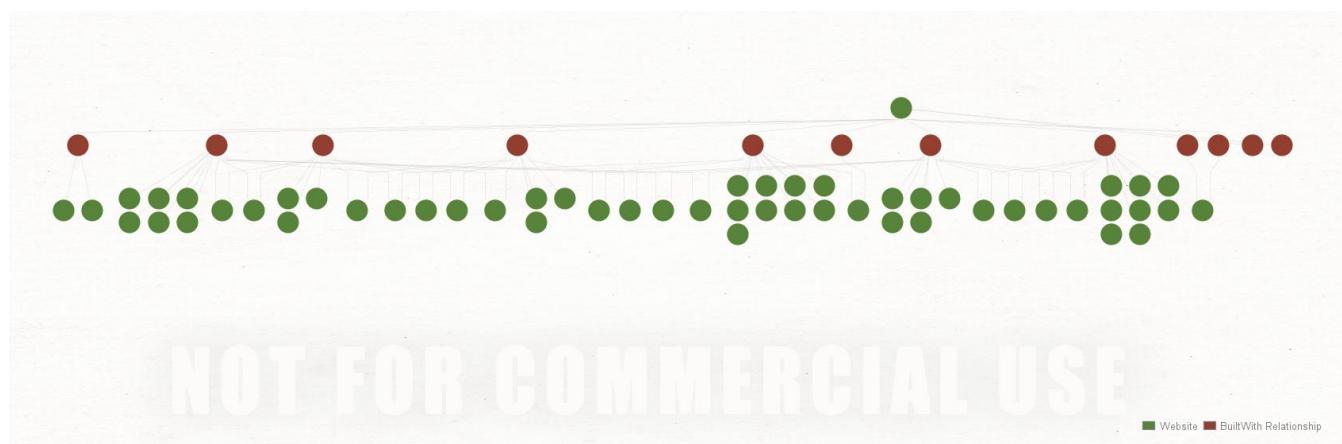
Ảnh kết quả (có đính kèm file chi tiết).

b. Ta tạo website “www.uit.edu.vn” → chuột phải, chọn run trên transform “Website Relationships”



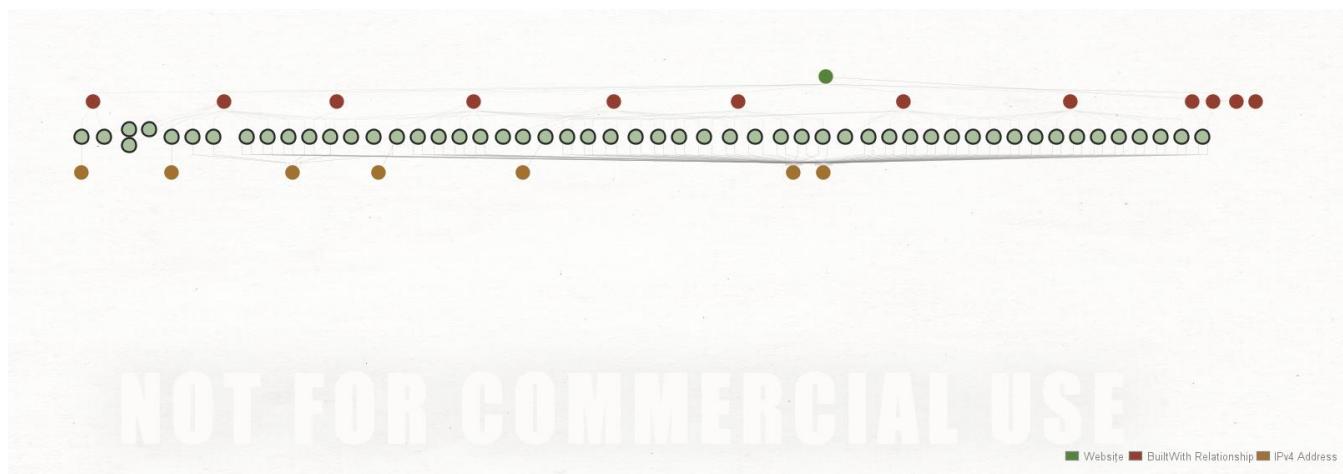
Ảnh các ip.

Tiếp theo, chọn tất cả ip hiện ra → chuột phải, chọn run trên transform “Get Websites” → Các website liên quan sẽ hiện ra.



Ảnh mô hình các website liên quan (có đính kèm file chi tiết).

Sau đó, ta chọn tất cả các website vừa mới xuất hiện → chuột phải → chọn “All transforms” → chọn run trên “To IP Address [DNS]” → IP ứng với từng website sẽ hiện lên.



Ảnh khái quát ip tương ứng của từng website (có đính kèm file chi tiết).

Câu 21: Ngoài các bản ghi kể trên, hãy liệt kê các bản ghi khác của DNS.

Trả lời:

- Các bản ghi đã được liệt kê ở trên như : NS, A, MX, PTR, CNAME, TXT
 - Ngoài ra còn có các bản ghi phổ biến :
 - AAAA: Là loại bản ghi được dùng để ánh xạ một tên miền thành đại chỉ Ipv6
 - SOA: Lưu trữ các thông tin admin về tên miền. Bao gồm các thông tin như tên máy chủ chính quản lý tên miền, địa chỉ email của người quản lý, phiên bản tên miền, thời gian làm mới, và nhiều thông tin khác liên quan đến quản lý tên miền.
 - SRV: chứa các thông tin như tên dịch vụ, tên miền, port và độ ưu tiên, giúp các ứng dụng tìm và kết nối đến máy chủ chứa dịch vụ cần thiết.
 - Các bản ghi ít phổ biến hơn như :
 - APL: Quản lý chỉ định 1 dải các ip address
 - DNAME: Ngoài việc tạo ra các bí danh (alias) như CNAME thì nó còn điều hướng các tên miền phụ trỏ đến 1 tên miền khác
 - HIP: Phân tách vai trò của một địa chỉ IP, thường dùng trong mobile computing
- LOC: Chứa thông tin địa lý cho tên miền về kinh độ và vĩ độ.

Câu 22: Sử dụng lệnh host để tìm kiếm các bản ghi TXT, MX cho tên miền uit.edu.vn

Trả lời:

```
(kali㉿kali)-[~]
└─$ host -t txt uit.edu.vn
uit.edu.vn descriptive text "MS=E431E3CA3EFF5A6431E2378C924984A8A0334ABC"
uit.edu.vn descriptive text "sqm6y27vn74pm290pl0fq4hcr08gst5r"
uit.edu.vn descriptive text "svp60rjlwr6s19rn9t013cfwm3xmqx7h"
uit.edu.vn descriptive text "v=spf1 include:_spf.google.com ~all"
uit.edu.vn descriptive text "google-site-verification=wjArKGa37oHK083XqT2C91tPny8NLttGS0aU5pJjKiY"

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

Câu 25: Viết một chương trình Bash script để liệt kê danh sách các nameserver của các đơn vị thành viên thuộc Đại học Quốc Gia TP.HCM (hcmus.edu.vn, hcmussh.edu.vn, uit.edu.vn, hcmut.edu.vn, hcmiu.edu.vn, uel.edu.vn, hcmier.edu.vn, vnuhcm.edu.vn) và thực hiện zone transfer ứng với các nameserver đã tìm được.

Trả lời:

```
An_toan_mang > code > lab2-25.sh
1  #!/bin/bash
2
3  domains=("hcmus.edu.vn" "hcmussh.edu.vn" "uit.edu.vn" "hcmut.edu.vn" "hcmiu.edu.vn" "uel.edu.vn" "hcmier.edu.vn" "vnuhcm.edu.vn")
4
5  for domain in "${domains[@]}"; do
6      echo "Domain: $domain"
7
8      for nameServer in $(host -t ns "$domain" 2> /dev/null | cut -d " " -f 4); do
9          echo "Name Server: $nameServer"
10         echo "Zone Transfer"
11
12         result=$(host -l "$domain" "$nameServer" 2> /dev/null)
13
14         if [ $? -eq 0 ]; then
15             echo "Zone transfer successful:"
16             echo "$result"
17         else
18             echo "Zone transfer failed"
19         fi
20
21         echo "-----"
22     done
23
24     echo "//////////"
25 done
```

- **Kết quả:**

```
(kali㉿kali)-[~]
$ ./script-25-lab2.sh
Domain: hcmus.edu.vn
Name Server: dns2.hcmus.edu.vn.
Zone Transfer
Zone transfer failed
-----
Name Server: dns1.hcmus.edu.vn.
Zone Transfer
Zone transfer failed
-----
Name Server: server.hcmus.edu.vn.
Zone Transfer
Zone transfer failed
-----
Domain: hcmussh.edu.vn
Name Server: server.vnuhcm.edu.vn.
Zone Transfer
Zone transfer failed
-----
Name Server: vnuserserv.vnuhcm.edu.vn.
Zone Transfer
Zone transfer failed
-----
Domain: uit.edu.vn
Name Server: nsbak.pavietnam.net.
Zone Transfer
Zone transfer failed
-----
Name Server: ns1.pavietnam.vn.
Zone Transfer
Zone transfer failed
-----
Name Server: ns2.pavietnam.vn.
Zone Transfer
Zone transfer failed
```

```
///////////////////////////// 168.45.128      192.168.45.140      TCP    74
Domain: hcmut.edu.vn          192.168.45.140      192.168.45.128      TCP    74
Name Server: dns1.hcmut.edu.vn. 192.168.45.128      192.168.45.140      TCP    66
Zone Transfer 707447767 192.168.45.128      192.168.45.140      TCP    66
Zone transfer failed

Name Server: dns3.hcmut.edu.vn.
Zone Transfer
Zone transfer failed

Name Server: dns2.hcmut.edu.vn.
Zone Transfer
Zone transfer failed

Name Server: dns4.hcmut.edu.vn.
Zone Transfer
Zone transfer failed

///////////////////////////// Domain: hcmiu.edu.vn
Name Server: hcm-server1.vnn.vn.
Zone Transfer
Zone transfer failed

Name Server: vdc-hn01.vnn.vn.
Zone Transfer
Zone transfer failed

///////////////////////////// Domain: uel.edu.vn
Name Server: ns2.dns.net.vn.
Zone Transfer
Zone transfer failed

Name Server: ns1.dns.net.vn.
Zone Transfer
Zone transfer failed

///////////////////////////// Domain: hcmier.edu.vn
Name Server: server.vnuhcm.edu.vn.
Zone Transfer
Zone transfer failed

Name Server: vnuserv.vnuhcm.edu.vn.
Zone Transfer
Zone transfer failed
```

```
///////////////
Domain: vnuhcm.edu.vn      Source          Destination
Name Server: ns2.vdc2.vn.    192.168.45.128   192.168.45.140
Zone Transfer
Zone transfer successful: 192.168.45.140   192.168.45.128
Using domain server: 103.192.168.45.128   192.168.45.140
Name: ns2.vdc2.vn.47767 192.168.45.128   192.168.45.140
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
baixekev.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.cnttt.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
gddhoinhapquocte.vnuhcm.edu.vn has address 123.30.191.189
Packets: 2085 - Disp
```

```
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
khcn.vnuhcm.edu.vn has address 203.162.147.185
quanly.khcn.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
kitucxa.vnuhcm.edu.vn has address 45.117.77.102
ksknsvtn.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
qldt.vnuhcm.edu.vn has address 103.88.121.38
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
tapchikhoaohoc.vnuhcm.edu.vn has address 203.162.147.185
```

```

tapchikhoaoc.vnuhcm.edu.vn has address 203.162.147.185 58.45.140      TCP
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
ttddt.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

Name Server: server.vnuhcm.edu.vn.
Zone Transfer
Zone transfer failed

Name Server: ns1.vdc2.vn.
Zone Transfer
Zone transfer failed

Name Server: vnuserv.vnuhcm.edu.vn.
Zone Transfer
Zone transfer failed

///////////

```

Câu 26: Viết Liệt kê danh sách các loại enumeration có thể được sử dụng cùng với tùy chọn -t

Trả lời : Ta có thể dùng lệnh **man dnsrecon** để check xem

```

-t TYPE, --type TYPE
  Type of enumeration to perform. There are several possible types:
  • std: SOA, NS, A, AAAA, MX and SRV.
  • rvl: Reverse lookup of a given CIDR or IP range.
  • btr: Brute force domains and hosts using a given dictionary.
  • srv: SRV records.
  • axfr: Test all NS servers for a zone transfer.
  • bing: Perform Bing search for subdomains and hosts.
  • yand: Perform Yandex search for subdomains and hosts.
  • crt: Perform crt.sh search for subdomains and hosts.
  • snoop: Perform cache snooping against all NS servers for a given domain, testing all with file containing the domains, file given with -D option.
  • tld: Remove the TLD of given domain and test against all TLDs registered in IANA.
  • zonewalk: Perform a DNSSEC zone walk using NSEC records.

  Host is up (0.0021s latency).
  Net: shown: 977 closed/0 ports (conn-refused)
  PORT      STATE SERVICE
  22/tcp    open  ssh
  22/tcp    open  telnet
  23/tcp    open  smtp
  53/tcp    open  domain
  80/tcp    open  http
  113/tcp   open  rpbinding
  139/tcp   open  netbios-ssn
  445/tcp   open  microsoft-ds
  512/tcp   open  exec
  513/tcp   open  login
  516/tcp   open  shell
  1099/tcp  open  rmiregistry
  1324/tcp  open  ingreslock
  2049/tcp  open  nfs
  2323/tcp  open  ccproxxy-ftp
  5432/tcp  open  postgresql
  5900/tcp  open  vnc
  6000/tcp  open  x11
  8080/tcp  open  http

```

Câu 27: Cho một vài ví dụ sử dụng kết hợp các tùy chọn được DNSRecon hỗ trợ khác (ít nhất là 2 ví dụ)

Trả lời:

- Reverse Lookup:

```
(kali㉿kali)-[~]
└─$ dnsrecon -r 208.67.222.200-208.67.222.255 -d microsoft.com
[*] Performing Reverse Lookup from 208.67.222.200 to 208.67.222.255
[+] PTR resolver1.opendns.com 208.67.222.222
[+] PTR dns.umbrella.com 208.67.222.222
[+] PTR dns.opendns.com 208.67.222.222
[+] PTR resolver3.opendns.com 208.67.222.220
[+] 4 Records Found
```

- Cache snooping:

```
(kali㉿kali)-[~/an-ninh-mang]
└─$ ls
list.txt  script-25-lab2

(kali㉿kali)-[~/an-ninh-mang]
└─$ dnsrecon -t snoop -n NS3.MEGACORPONE.COM -d megacorpone.com -D list.txt
[*] Using the dictionary file: list.txt (provided by user)
[*] snoop: Performing Cache Snooping against NS Server: 66.70.207.180 ...
[*]     Name: localhost. TTL: 604800 Address: 127.0.0.1 Type: A
    Wireshark _eth0MLTNC2.pcapng : Packets: 2085 · Displayed: 4 (0.2%)
```

Câu 28: So sánh 2 công cụ DNSEnum và DNSRecon? Công cụ nào dễ sử dụng hơn?

Công cụ nào cho kết quả chính xác hơn? Công cụ nào hiển thị nhiều kết quả hơn?

Trả lời:

- Độ dễ sử dụng:
 - DNSRecon: DNSRecon thường được coi là dễ sử dụng hơn. Nó cung cấp một giao diện dòng lệnh đơn giản và có các tùy chọn dễ hiểu.
 - DNSEnum: DNSEnum có một số tùy chọn phức tạp hơn so với DNSRecon.
- Kết quả chính xác:
 - Cả hai công cụ đều có thể cung cấp kết quả chính xác nếu được sử dụng đúng cách.
- Số lượng kết quả:
 - DNSRecon: DNSRecon cho phép thực hiện nhiều loại enumeration và thu thập

nhiều loại thông tin, bao gồm subdomains, MX records, SRV records, và nhiều bản ghi khác. Điều này có nghĩa rằng DNSRecon có khả năng hiển thị nhiều kết quả hơn về tên miền mục tiêu.

- DNSEnum: DNSEnum cũng có khả năng thu thập nhiều thông tin về tên miền mục tiêu, nhưng phải được cấu hình cẩn thận để có kết quả tốt.

Câu 29: Thực hiện bắt Wireshark để mô tả cách gói tin được gửi và nhận khi thực hiện SYN Scan sử dụng Nmap

Trả lời:

- Ta có ip address của metasploitable2:

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 00:0c:29:92:0b:83  
          inet addr:192.168.45.140 Bcast:192.168.45.255 Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe92:b83/64 Scope:Link  
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
             RX packets:39 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:65 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:1000  
             RX bytes:4136 (4.0 KB) TX bytes:6826 (6.6 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:91 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:91 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:0  
             RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)  
msfadmin@metasploitable:~$
```

- Thực hiện scan ports:

```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.45.140
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-18 04:21 EDT
Nmap scan report for 192.168.45.140
Host is up (0.0011s 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:29:92:0B:83 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

- Bắt gói tin bằng wireshark

No.	Time	Source	Destination	Protocol	Length	Info
61	32.257952368	192.168.45.128	192.168.45.140	TCP	58	65196 -- 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
62	32.258008924	192.168.45.128	192.168.45.140	TCP	58	65196 -- 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
63	32.258061644	192.168.45.128	192.168.45.140	TCP	58	65196 -- 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
64	32.258118464	192.168.45.128	192.168.45.140	TCP	58	65196 -- 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
65	32.258177849	192.168.45.128	192.168.45.140	TCP	58	65196 -- 136 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
66	32.258227321	192.168.45.128	192.168.45.140	TCP	69	3306 -- 65196 [SYN, ACK] Seq=1 Ack=1 Win=540 Len=0 MSS=1460
67	32.258272365	192.168.45.128	192.168.45.140	TCP	54	65196 -- 3306 [RST] Seq=1 Win=0 Len=0
68	32.258332354	192.168.45.128	192.168.45.140	TCP	69	25 -- 65196 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
69	32.258544867	192.168.45.128	192.168.45.140	TCP	69	119 -- 65196 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
70	32.258544172	192.168.45.128	192.168.45.140	TCP	68	22 -- 65196 [SYN, ACK] Seq=9 Ack=1 Win=540 Len=0 MSS=1460
71	32.258544210	192.168.45.128	192.168.45.140	TCP	68	1723 -- 65196 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
72	32.258544259	192.168.45.128	192.168.45.140	TCP	69	443 -- 65196 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
73	32.258594633	192.168.45.128	192.168.45.140	TCP	54	65196 -- 22 [RST] Seq=1 Win=0 Len=0
74	32.258688679	192.168.45.128	192.168.45.140	TCP	69	8886 -- 65196 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75	32.258688767	192.168.45.128	192.168.45.140	TCP	69	3389 -- 65196 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76	32.258916349	192.168.45.128	192.168.45.140	TCP	69	135 -- 65196 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
77	32.258973441	192.168.45.128	192.168.45.140	TCP	69	100 -- 65100 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
78	32.258973173	192.168.45.128	192.168.45.140	TCP	58	65196 -- 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
79	32.259043168	192.168.45.128	192.168.45.140	TCP	58	65196 -- 919 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
80	32.259115836	192.168.45.128	192.168.45.140	TCP	58	65196 -- 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
81	32.259194187	192.168.45.128	192.168.45.140	TCP	58	65196 -- 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
Frame 1: 237 bytes on wire (1736 bits), 237 bytes captured (1736 bits) on interface eth0, id 0						
Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)						
Internet Protocol Version 4, Src: 192.168.45.128, Dst: 193.255.255.250						
User Datagram Protocol, Src Port: 57620, Dst Port: 1980						
Simple Service Discovery Protocol						
Frame 2: 237 bytes on wire (1736 bits), 237 bytes captured (1736 bits) on interface eth0, id 1						
Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)						
Internet Protocol Version 4, Src: 192.168.45.128, Dst: 193.255.255.250						
User Datagram Protocol, Src Port: 57620, Dst Port: 1980						
Simple Service Discovery Protocol						
Frame 3: 237 bytes on wire (1736 bits), 237 bytes captured (1736 bits) on interface eth0, id 2						
Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)						
Internet Protocol Version 4, Src: 192.168.45.128, Dst: 193.255.255.250						
User Datagram Protocol, Src Port: 57620, Dst Port: 1980						
Simple Service Discovery Protocol						

- Trường hợp port đang mở:
 - Đầu tiên thì máy ta sẽ gửi gói tin SYN đến yêu cầu kết nối TCP
 - Máy mục tiêu sẽ gửi lại gói SYN, ACK để cho biết rằng nó đã sẵn sàng thiết lập kết nối, tức là nó đã mở cổng rồi.
 - Cuối cùng ta gửi gói RST để chấm dứt kết nối TCP một cách đột ngột. Do là lúc này ta biết nó đã mở cổng đó rồi.

tcp.port == 22						
No.	Time	Source	Destination	Protocol	Length	Info
59	32.257840549	192.168.45.128	192.168.45.140	TCP	58	65196 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
70	32.258544172	192.168.45.140	192.168.45.128	TCP	60	22 → 65196 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
73	32.258594635	192.168.45.128	192.168.45.140	TCP	54	65196 → 22 [RST] Seq=1 Win=0 Len=0

- Trường hợp port đang đóng:
 - Tương tự như trên đầu tiên ta cũng gửi gói SYN đến để yêu cầu 1 kết nối TCP.
 - Máy đích trả lại cho ta gói RST, ACK cho thấy là máy đích ở port đó đang không hoạt động, dẫn đến không thể thiết lập kết nối

tcp.port == 9999						
No.	Time	Source	Destination	Protocol	Length	Info
641	32.284567824	192.168.45.128	192.168.45.140	TCP	58	65196 → 9999 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
668	32.285131877	192.168.45.140	192.168.45.128	TCP	60	9999 → 65196 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Câu 31: So sánh với sử dụng phương thức SYN Scan (số lượng gói tin được gửi, số lượng

gói tin được nhận, thời gian quét, kết quả hiển thị...)

Trả lời:

✍ TCP Connect Scan:

- Số gói tin gửi đi:

No.	Time	Source	Destination	Protocol	Length	Info
1940	0.069640969	192.168.45.128	192.168.45.140	TCP	74	46386 → 8443 [SYN] Seq=0
1941	0.069672408	192.168.45.128	192.168.45.140	TCP	74	51110 → 7004 [SYN] Seq=0
1942	0.069695434	192.168.45.128	192.168.45.140	TCP	74	46440 → 9099 [SYN] Seq=0
1943	0.069726932	192.168.45.128	192.168.45.140	TCP	74	58994 → 2022 [SYN] Seq=0
1944	0.069751261	192.168.45.128	192.168.45.140	TCP	74	36504 → 6101 [SYN] Seq=0
1945	0.069782900	192.168.45.128	192.168.45.140	TCP	74	55782 → 1053 [SYN] Seq=0
1946	0.069806053	192.168.45.128	192.168.45.140	TCP	74	43064 → 32778 [SYN] Seq=0
1947	0.069836732	192.168.45.128	192.168.45.140	TCP	74	56658 → 9091 [SYN] Seq=0
1948	0.069859984	192.168.45.128	192.168.45.140	TCP	74	50528 → 1072 [SYN] Seq=0
1949	0.069891527	192.168.45.128	192.168.45.140	TCP	74	53040 → 563 [SYN] Seq=0 W
1950	0.069915207	192.168.45.128	192.168.45.140	TCP	74	35634 → 5200 [SYN] Seq=0
1951	0.069943922	192.168.45.128	192.168.45.140	TCP	74	34562 → 3827 [SYN] Seq=0
1968	0.070212662	192.168.45.128	192.168.45.140	TCP	66	39924 → 8180 [ACK] Seq=1
1969	0.070245965	192.168.45.128	192.168.45.140	TCP	66	39924 → 8180 [RST, ACK] S
1970	0.070315604	192.168.45.128	192.168.45.140	TCP	74	57864 → 35500 [SYN] Seq=0
1971	0.070350770	192.168.45.128	192.168.45.140	TCP	74	51494 → 4125 [SYN] Seq=0
1972	0.070373726	192.168.45.128	192.168.45.140	TCP	74	58270 → 1044 [SYN] Seq=0
1973	0.070405144	192.168.45.128	192.168.45.140	TCP	74	38380 → 5280 [SYN] Seq=0
1974	0.070428254	192.168.45.128	192.168.45.140	TCP	74	39832 → 7435 [SYN] Seq=0
1975	0.070457198	192.168.45.128	192.168.45.140	TCP	74	40940 → 1060 [SYN] Seq=0
1984	0.070480321	192.168.45.128	192.168.45.140	TCP	74	60554 → 8022 [SYN] Seq=0
1987	0.070509704	192.168.45.128	192.168.45.140	TCP	74	59634 → 1058 [SYN] Seq=0
1988	0.070536854	192.168.45.128	192.168.45.140	TCP	74	41152 → 3851 [SYN] Seq=0
1989	0.070565947	192.168.45.128	192.168.45.140	TCP	74	41900 → 6502 [SYN] Seq=0
1990	0.070588566	192.168.45.128	192.168.45.140	TCP	74	52420 → 49153 [SYN] Seq=0

Frame 1: 74 bytes on wire (592 bits), 74 bytes cap
 Ethernet II, Src: VMware_d6:1e:af (00:0c:29:d6:1e:
 Internet Protocol Version 4, Src: 192.168.45.128,
 Transmission Control Protocol, Src Port: 35742, Ds

0000	00 0c 29 92 0b 83 00 0c 29 d6 1e af 08 00 45
0010	00 3c b0 52 40 00 40 06 ae 0c c0 a8 2d 80 c0
0020	2d 8c 8b 9e 00 50 2c 53 45 9c 00 00 00 00 a0
0030	fa f0 dc 8b 00 00 02 04 05 b4 04 02 08 0a 0f
0040	96 52 00 00 00 00 01 03 03 07

- Số gói tin nhận được:

No.	Time	Source	Destination	Protocol	Length	Info
2036	0.071587825	192.168.45.140	192.168.45.128	TCP	60	1061 → 57468 [RST, ACK] S
2037	0.071587874	192.168.45.140	192.168.45.128	TCP	60	5120 → 38590 [RST, ACK] S
2038	0.071587929	192.168.45.140	192.168.45.128	TCP	60	8443 → 46386 [RST, ACK] S
2039	0.071587980	192.168.45.140	192.168.45.128	TCP	60	9099 → 51110 [RST, ACK] S
2040	0.071588027	192.168.45.140	192.168.45.128	TCP	60	9099 → 46440 [RST, ACK] S
2041	0.071838879	192.168.45.140	192.168.45.128	TCP	60	2022 → 58994 [RST, ACK] S
2042	0.071838951	192.168.45.140	192.168.45.128	TCP	60	6101 → 36504 [RST, ACK] S
2043	0.071838998	192.168.45.140	192.168.45.128	TCP	60	1053 → 55782 [RST, ACK] S
2044	0.071839047	192.168.45.140	192.168.45.128	TCP	60	32778 → 43064 [RST, ACK]
2045	0.071839090	192.168.45.140	192.168.45.128	TCP	60	9091 → 56658 [RST, ACK] S
2046	0.071839134	192.168.45.140	192.168.45.128	TCP	60	1072 → 50528 [RST, ACK] S
2047	0.071839182	192.168.45.140	192.168.45.128	TCP	60	563 → 53040 [RST, ACK] S
2048	0.071839231	192.168.45.140	192.168.45.128	TCP	60	5200 → 35634 [RST, ACK] S
2049	0.071893310	192.168.45.140	192.168.45.128	TCP	60	3827 → 34562 [RST, ACK] S
2050	0.071893398	192.168.45.140	192.168.45.128	TCP	60	35500 → 57864 [RST, ACK]
2051	0.071893456	192.168.45.140	192.168.45.128	TCP	60	4125 → 51494 [RST, ACK] S
2052	0.071893501	192.168.45.140	192.168.45.128	TCP	60	1044 → 58270 [RST, ACK] S
2053	0.071893552	192.168.45.140	192.168.45.128	TCP	60	5280 → 38380 [RST, ACK] S
2054	0.071893605	192.168.45.140	192.168.45.128	TCP	60	7435 → 39832 [RST, ACK] S
2055	0.071893652	192.168.45.140	192.168.45.128	TCP	60	1060 → 40940 [RST, ACK] S
2056	0.071893695	192.168.45.140	192.168.45.128	TCP	60	8022 → 60554 [RST, ACK] S
2057	0.073727246	192.168.45.140	192.168.45.128	TCP	60	1058 → 59634 [RST, ACK] S
2058	0.073727317	192.168.45.140	192.168.45.128	TCP	60	3851 → 41152 [RST, ACK] S
2059	0.073727366	192.168.45.140	192.168.45.128	TCP	60	6502 → 41900 [RST, ACK] S
2060	0.073727415	192.168.45.140	192.168.45.128	TCP	60	49153 → 52420 [RST, ACK]

- Giao diện hiển thị:

```
(kali㉿kali)-[~]
$ nmap -sT 192.168.45.140
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-18 04:45 EDT
Nmap scan report for 192.168.45.140
Host is up (0.0033s 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

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

⊕ TCP SYN Scan:

- Số gói tin gửi đi:

No.	Time	Source	Destination	Protocol	Length	Info
1975	13.171815769	192.168.45.128	192.168.45.140	TCP	58	60001 → 2161 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1976	13.171831708	192.168.45.128	192.168.45.140	TCP	58	60001 → 8192 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1977	13.171889758	192.168.45.128	192.168.45.140	TCP	58	60001 → 18988 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1978	13.171904773	192.168.45.128	192.168.45.140	TCP	58	60001 → 2020 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1979	13.171963055	192.168.45.128	192.168.45.140	TCP	58	60001 → 50630 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1980	13.171978878	192.168.45.128	192.168.45.140	TCP	58	60001 → 5811 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1981	13.172037323	192.168.45.128	192.168.45.140	TCP	58	60001 → 5906 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1982	13.172052381	192.168.45.128	192.168.45.140	TCP	58	60001 → 8899 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1983	13.172111245	192.168.45.128	192.168.45.140	TCP	58	60001 → 6567 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1984	13.172126847	192.168.45.128	192.168.45.140	TCP	58	60001 → 1524 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1985	13.172184942	192.168.45.128	192.168.45.140	TCP	58	60001 → 32778 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1986	13.172200432	192.168.45.128	192.168.45.140	TCP	58	60001 → 2030 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1987	13.172259756	192.168.45.128	192.168.45.140	TCP	58	60001 → 5414 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1988	13.172274726	192.168.45.128	192.168.45.140	TCP	58	60001 → 631 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1989	13.172336327	192.168.45.128	192.168.45.140	TCP	58	60001 → 2179 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1990	13.172385233	192.168.45.128	192.168.45.140	TCP	58	60001 → 714 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2004	13.172492726	192.168.45.128	192.168.45.140	TCP	58	60001 → 2119 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2005	13.172508458	192.168.45.128	192.168.45.140	TCP	58	60001 → 43 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2006	13.172568144	192.168.45.128	192.168.45.140	TCP	58	60001 → 5221 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2007	13.172586868	192.168.45.128	192.168.45.140	TCP	58	60001 → 32781 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2008	13.172658474	192.168.45.128	192.168.45.140	TCP	58	60001 → 1148 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2009	13.172678072	192.168.45.128	192.168.45.140	TCP	58	60001 → 3003 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2010	13.172748310	192.168.45.128	192.168.45.140	TCP	58	60001 → 1369 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2011	13.172764248	192.168.45.128	192.168.45.140	TCP	58	60001 → 7625 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2020	13.173043560	192.168.45.128	192.168.45.140	TCP	54	60001 → 1524 [RST] Seq=1 Win=0 Len=0

- Số gói tin nhận được:

ip.src==192.168.45.140 && ip.dst==192.168.45.128						
No.	Time	Source	Destination	Protocol	Length	Info
1997	13.172438157	192.168.45.140	192.168.45.128	TCP	60	787 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1998	13.172438197	192.168.45.140	192.168.45.128	TCP	60	2161 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1999	13.172466552	192.168.45.140	192.168.45.128	TCP	60	8192 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2000	13.172466621	192.168.45.140	192.168.45.128	TCP	60	18988 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2001	13.172466662	192.168.45.140	192.168.45.128	TCP	60	2020 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2002	13.172466704	192.168.45.140	192.168.45.128	TCP	60	50636 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2003	13.172466745	192.168.45.140	192.168.45.128	TCP	60	5811 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2012	13.173015344	192.168.45.140	192.168.45.128	TCP	60	5906 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2013	13.173015419	192.168.45.140	192.168.45.128	TCP	60	8899 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2014	13.173015466	192.168.45.140	192.168.45.128	TCP	60	6567 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2015	13.173015513	192.168.45.140	192.168.45.128	TCP	60	1524 → 60001 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
2016	13.173015552	192.168.45.140	192.168.45.128	TCP	60	32778 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2017	13.173015592	192.168.45.140	192.168.45.128	TCP	60	2030 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2018	13.173015630	192.168.45.140	192.168.45.128	TCP	60	5414 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2019	13.173015670	192.168.45.140	192.168.45.128	TCP	60	631 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2021	13.173067807	192.168.45.140	192.168.45.128	TCP	60	2179 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2022	13.173067883	192.168.45.140	192.168.45.128	TCP	60	714 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2023	13.173067923	192.168.45.140	192.168.45.128	TCP	60	2119 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2024	13.173067970	192.168.45.140	192.168.45.128	TCP	60	43 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2025	13.173068015	192.168.45.140	192.168.45.128	TCP	60	5221 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2026	13.173068060	192.168.45.140	192.168.45.128	TCP	60	32781 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2027	13.175399764	192.168.45.140	192.168.45.128	TCP	60	1148 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2028	13.175399961	192.168.45.140	192.168.45.128	TCP	60	3003 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2029	13.175400004	192.168.45.140	192.168.45.128	TCP	60	1309 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2030	13.175400045	192.168.45.140	192.168.45.128	TCP	60	7625 → 60001 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

○ Giao diện hiển thị:

```

[sudo] su
[root@kali]# nmap -sS 192.168.45.140
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-18 04:45 EDT
Nmap scan report for 192.168.45.140
Host is up (0.00059s 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:29:92:0B:83 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

```

So sánh:

Phương thức quét	TCP Connect Scan	TCP SYN Scan
Số lượng gói tin gửi	1990	2020
Số lượng gói tin nhận	2060	2030

Thời gian quét	0.11s	0.28s
Giao diện hiển thị	Không có MAC addr của máy mục tiêu	Có MAC addr của máy mục tiêu

Câu 32: Thực hiện kiểm tra các host đang hoạt động trong mạng bằng các ngôn ngữ lập trình khác (Bash script, Python, C/C++, Perl, ...)

Trả lời:

```
An_toan_mang > code > lab2 > lab2-host-up.py > ...
1  import subprocess
2
3  base_ip = "192.168.45."
4
5
6  def ping_host(ip):
7      try:
8          result = subprocess.check_output(["ping", "-c", "2", ip])
9          return True
10     except subprocess.CalledProcessError:
11         return False
12
13
14 for i in range(1, 255):
15     ip = base_ip + str(i)
16
17 if ping_host(ip):
18     print(f"{ip} is up")
19
```

- Kết quả:

```
(kali㉿kali)-[~/an-ninh-mang]
$ python3 host-up.py
192.168.45.2 is up
192.168.45.128 is up
192.168.45.140 is up
```

Câu 33: Sử dụng Wireshark để phân tích gói tin khi sử dụng Nmap với tùy chọn -sn

Trả lời:

```
(kali㉿kali)-[~/an-ninh-mang]
$ nmap -v -sn 192.168.45.1-254
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-18 05:32 EDT
Initiating Ping Scan at 05:32
Scanning 254 hosts [2 ports/host]
Completed Ping Scan at 05:32, 3.00s elapsed (254 total hosts)
Initiating Parallel DNS resolution of 3 hosts. at 05:32
Completed Parallel DNS resolution of 3 hosts. at 05:32, 0.04s elapsed
Nmap scan report for 192.168.45.1 [host down]
Nmap scan report for 192.168.45.2
Host is up (0.00068s latency).
Nmap scan report for 192.168.45.3 [host down]
Nmap scan report for 192.168.45.4 [host down]
Nmap scan report for 192.168.45.5 [host down]
Nmap scan report for 192.168.45.6 [host down]
Nmap scan report for 192.168.45.7 [host down]
Nmap scan report for 192.168.45.8 [host down]
Nmap scan report for 192.168.45.9 [host down]
Nmap scan report for 192.168.45.10 [host down]
Nmap scan report for 192.168.45.11 [host down]
Nmap scan report for 192.168.45.12 [host down]
Nmap scan report for 192.168.45.13 [host down]
Nmap scan report for 192.168.45.14 [host down]
Nmap scan report for 192.168.45.15 [host down]
Nmap scan report for 192.168.45.16 [host down]
Nmap scan report for 192.168.45.17 [host down]
Nmap scan report for 192.168.45.18 [host down]
Nmap scan report for 192.168.45.19 [host down]
Nmap scan report for 192.168.45.20 [host down]
Nmap scan report for 192.168.45.21 [host down]
Nmap scan report for 192.168.45.22 [host down]
Nmap scan report for 192.168.45.125 [host down]
Nmap scan report for 192.168.45.126 [host down]
Nmap scan report for 192.168.45.127 [host down]
Nmap scan report for 192.168.45.128
Host is up (0.0011s latency).
Nmap scan report for 192.168.45.129 [host down]
Nmap scan report for 192.168.45.130 [host down]
Nmap scan report for 192.168.45.131 [host down]
Nmap scan report for 192.168.45.132 [host down]
Nmap scan report for 192.168.45.133 [host down]
Nmap scan report for 192.168.45.134 [host down]
Nmap scan report for 192.168.45.135 [host down]
Nmap scan report for 192.168.45.136 [host down]
Nmap scan report for 192.168.45.137 [host down]
Nmap scan report for 192.168.45.138 [host down]
Nmap scan report for 192.168.45.139 [host down]
Nmap scan report for 192.168.45.140
Host is up (0.017s latency).
Nmap scan report for 192.168.45.141 [host down]
Nmap scan report for 192.168.45.142 [host down]
Nmap scan report for 192.168.45.143 [host down]
Nmap scan report for 192.168.45.144 [host down]
Nmap scan report for 192.168.45.145 [host down]
```

- Wireshark:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.2? Tell 192.168.45.128
2	0.000157003	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.3? Tell 192.168.45.128
3	0.000214559	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.4? Tell 192.168.45.128
4	0.000245940	VMware_e9:af:fa	VMware_d6:1e:af	ARP	60	192.168.45.2 is at 00:50:56:e9:af:fa
5	0.000254320	192.168.45.128	192.168.45.2	TCP	74	46180 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSV
6	0.000282686	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.5? Tell 192.168.45.128
7	0.000283867	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.6? Tell 192.168.45.128
8	0.000362488	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.7? Tell 192.168.45.128
9	0.000385244	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.8? Tell 192.168.45.128
10	0.000435279	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.9? Tell 192.168.45.128
11	0.000491162	192.168.45.2	192.168.45.128	TCP	60	80 → 46180 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
12	0.000502785	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.10? Tell 192.168.45.128
13	0.000544181	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.11? Tell 192.168.45.128
14	0.000686704	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.14? Tell 192.168.45.128
15	0.000747296	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.15? Tell 192.168.45.128
16	0.101166409	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.18? Tell 192.168.45.128
17	0.101372299	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.19? Tell 192.168.45.128
18	0.101473948	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.20? Tell 192.168.45.128
19	0.101553509	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.21? Tell 192.168.45.128
20	0.101596372	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.22? Tell 192.168.45.128
21	0.101682556	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.23? Tell 192.168.45.128
22	0.101802371	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.24? Tell 192.168.45.128
23	0.101844963	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.25? Tell 192.168.45.128
24	0.101912450	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.26? Tell 192.168.45.128
25	0.101971485	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.27? Tell 192.168.45.128
26	0.102028660	VMware_d6:1e:af	Broadcast	ARP	42	Who has 192.168.45.28? Tell 192.168.45.128
Frame 199: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0						
Ethernet II, Src: VMware_d6:1e:af (00:0c:29:06:1e:af), Dst: VMware_92:0b:83 (00:0c:29:92:0b:83)						
Internet Protocol Version 4, Src: 192.168.45.128, Dst: 192.168.45.128						
Transmission Control Protocol, Src Port: 51820, Dst Port: 80, Seq: 0, Len: 0						
0000 00 0c 29 92 0b 83 00 0c 29 0010 00 3c ae f8 40 00 40 06 af 0020 2d 8c ca 6c 00 50 cb 92 92 0030 fa f0 dc 8b 00 00 02 04 05 0040 3d 89 00 00 00 00 01 03 03						

- Những host đang hoạt động sẽ gửi phản hồi lại:

ip.dst==192.168.45.128						
No.	Time	Source	Destination	Protocol	Length	Info
11	0.000491162	192.168.45.2	192.168.45.128	TCP	60	80 → 46180 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
159	1.303717740	192.168.45.2	192.168.45.128	TCP	60	80 → 46190 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
294	1.306079112	192.168.45.140	192.168.45.128	TCP	74	80 → 51820 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 S/
578	2.604359083	192.168.45.140	192.168.45.128	TCP	74	80 → 51830 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 S/
637	3.006509099	192.168.45.2	192.168.45.128	DNS	166	Standard query response 0xce88 No such name PTR 140.45.168.1
638	3.006508463	192.168.45.2	192.168.45.128	DNS	166	Standard query response 0xce87 No such name PTR 128.45.168.1
650	3.050908427	192.168.45.2	192.168.45.128	DNS	164	Standard query response 0xce86 No such name PTR 2.45.168.192
783	15.464426239	192.168.45.254	192.168.45.128	DHCP	342	DHCP ACK - Transaction ID 0xc3c084c

Câu 34: Liệt kê các banner, dịch vụ đang chạy trên máy Metasploitable 2 (chỉ liệt kê các dịch vụ TCP).

Trả lời:

Dùng lệnh: nmap -sT -sV -A 192.168.45.140

Trong đó :

- sT: Đây là tùy chọn quét loại kết nối TCP SYN (SYN scan)
- sV: Đây là tùy chọn để xác định phiên bản của các dịch vụ mạng đang chạy trên máy chủ như (web server, SSH server, FTP server).
- A: Đây là tùy chọn để thực hiện một quét toàn diện (aggressive scan). Nmap sẽ kết hợp nhiều kiểu quét để thu thập thông tin chi tiết về máy chủ đích. Điều này bao gồm việc

xác định hệ điều hành, kiến thức về mạng, danh sách các cổng mạng mở, và việc xác định phiên bản của các dịch vụ mạng, và các lỗ hổng mà nó biết có trên dịch vụ đó

Kết quả:

```
[kali㉿kali:~] $ nmap -sT -sV -A 192.168.45.140
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-18 05:21 EDT
Nmap scan report for 192.168.45.140
Host is up (0.00085s latency).
Not 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_STAT:
|_FTP server status:
|   Connected to 192.168.45.128
|   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 500fcfe1c05f6a74d69024fac4d56cc (DSA)
|   2048 5656240f211de472bae51b1243de8f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ssl-date: 2023-10-18T09:22:33+00:00; +2s from scanner time.
|_smtp-commands: metasploitable.localdomain PIPELINING SIZE 10240000 VRFY ETRN STARTTLS ENHANCEDSTATUSCODES 8BITMIME DSN
|_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
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-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

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     44242/tcp mountd
|   100005  1,2,3     57200/udp mountd
|   100021  1,3,4     34210/tcp nlockmgr
|   100021  1,3,4     49686/udp nlockmgr
|   100024  1          40134/tcp status
|   100024  1          42095/udp status
|_ssl-date: 2023-10-18T09:22:33+00:00; +3s from scanner time.
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogin
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 #10003)
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: 13
|   Capabilities flags: 43564
|   Some Capabilities: Supports41Auth, SupportsTransactions, Speaks41ProtocolNew, SupportsCompression, SwitchToSSLAfterHandshake, LongColumnFlag, ConnectWithDatabase
|   Status: Autocommit
|_ Salt: 6[H8]{pg3..Mw20;vdo#
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-10-18T09:22:33+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, 1:05:31
|   source ident: nmap
|   source host: 1314F39B.15D434FA.FFFA6D49.IP
|   error: Closing Link: nlkuqzofa[192.168.45.128] (Quit: nlkuqzofa)
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-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|   System time: 2023-10-18T05:22:14-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_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: METASPOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.04 seconds

```

Câu 35: Sử dụng thêm 2 NSE script (tự chọn) để quét máy mục tiêu (Metasploitable 2)

Trả lời:

- **mysql-info:** Sẽ tiến hành thực hiện thu thập thông tin trên máy đích

```
(kali㉿kali)-[~/usr/share/nmap/scripts]$ nmap --script mysql-info 192.168.45.140
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-18 05:46 EDT
Nmap scan report for 192.168.45.140
Host is up (0.0017s 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
|_ mysql-info:
|  Protocol: 10
|  Version: 5.0.51a-3ubuntu5
|  Thread ID: 23
|  Capabilities flags: 43564
|  Some Capabilities: LongColumnFlag, Speaks41ProtocolNew, SwitchToSSLAfterHandshake, SupportsTransactions, ConnectWithDatabase, SupportsCompression, Support41Auth
|  Status: Autocommit
|_ Salt: %n"Z~b(?Cr6S}@e\[]!
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

- **nbstat**: được sử dụng để thực hiện kiểm tra NetBIOS Name Service (NBSTAT) trên máy đích

```
(kali㉿kali)-[~/usr/share/nmap/scripts]$ nmap --script nbstat 192.168.45.140
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-18 05:49 EDT
Nmap scan report for 192.168.45.140
Host is up (0.0014s latency).

Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh      (access denied)
23/tcp    open  telnet   UnrealIRCd
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

Host script results:
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| Names:
|_  METASPLOITABLE<00>  Flags: <unique><active>
|_  METASPLOITABLE<03>  Flags: <unique><active>
|_  METASPLOITABLE<20>  Flags: <unique><active>
|_  \x01\x02_MSBROWSE_\x02<01>  Flags: <group><active>
|_  WORKGROUP<00>  Flags: <group><active>
|_  WORKGROUP<1d>  Flags: <unique><active>
|_  WORKGROUP<1e>  Flags: <group><active>

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

YÊU CẦU CHUNG

- ∅ Sinh viên tìm hiểu và thực hành theo 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 **.DOCX** và **.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]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).

Ví dụ: [NT101.K11.ATCL]-Session1_Group3.

- ∅ 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 Lab.**
- ∅ Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- ∅ Chuẩn bị tốt.
- ∅ Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

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

HẾT