Bộ môn An toàn Thông tin – Khoa MMT&TT
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO BÀI TẬP

Môn học: An toàn mạng máy tính

Kỳ báo cáo: Buổi 02 (Session 02)

Tên chủ đề: Information Gathering

GV: Nghi Hoàng Khoa

Ngày báo cáo: 20/10/2022

Nhóm: 07 (nếu không có xoá phần này)

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT101.N11.ANTN

STT	Họ và tên	MSSV	Email
1	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn
2	Nguyễn Bảo Phương	20520704	20520704@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	35 câu hỏi	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

Câu 1:

Công ty hoạt động trong lĩnh vực công nghệ nano. Chịu trách nhiệm về xác định các tiêu chuẩn trong các lĩnh vực y tế, điện tử và thương mại.

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

Câu 2:

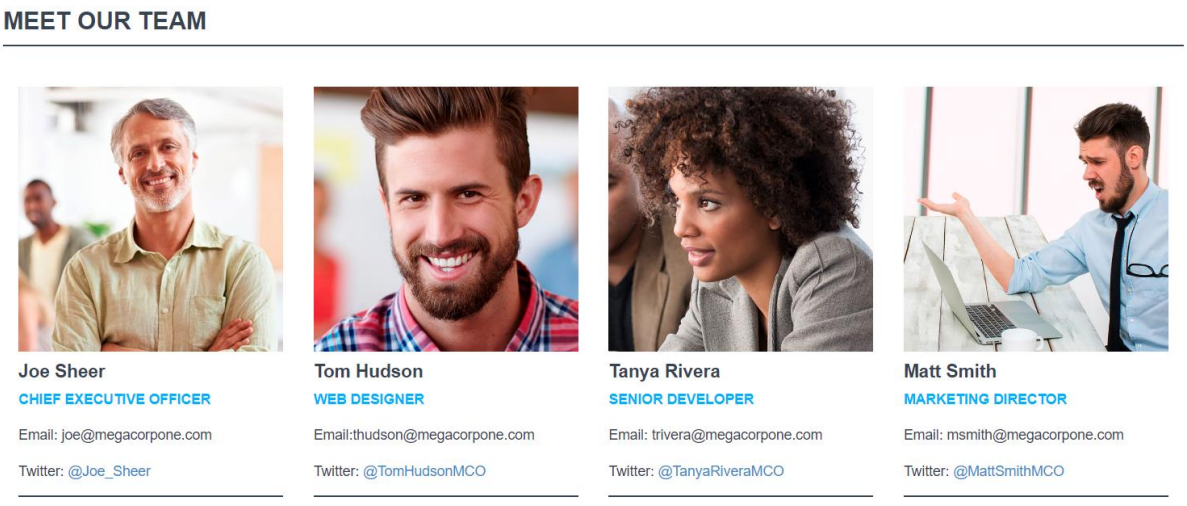
Những thành viên đang làm việc cho công ty MegaCorp One (Lấy từ trang MegaCorp One/About):

Joe Sheer, Chief Executive Office, email: joe@megacorpone.com, Twitter: @Joe_Sheer

Tom Hudson, Web Designer, email: thudson@megacorpone.com, Twitter: @TomHudsonMCO

Tanya Rivera, Senior Developer, email: trivera@megacorpone.com, Twitter: @TanyaRiveraMCO

Matt Smith, Marketing Director, email: msmith@megacorpone.com, Twitter: @MattSmithMCO



Câu 3

Email của các thành viên đang làm việc trong công ty MegaCorp One đều có company name domain (trong trường hợp này là @megacorpone.com) ở đuôi. Như vậy mọi thành viên đều có tên theo cú pháp <user>@megacorpone.com

Câu 4:

Xác định các name server của megacorpone.com:

Name server: NS1.MEGACORPONE.COM, NS2.MEGACORPONE.COM, NS3.MEGACORPONE

```
┌──(kali㉿kali)-[~]
└─$ whois megacorpone.com
   Domain Name: MEGACORPONE.COM
   Registry Domain ID: 1775445745_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.gandi.net
   Registrar URL: http://www.gandi.net
   Updated Date: 2022-06-14T18:01:06Z
   Creation Date: 2013-01-22T23:01:00Z
   Registry Expiry Date: 2024-01-22T23:01:00Z
   Registrar: Gandi SAS
   Registrar IANA ID: 81
   Registrar Abuse Contact Email: abuse@support.gandi.net
   Registrar Abuse Contact Phone: +33.170377661
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS1.MEGACORPONE.COM
   Name Server: NS2.MEGACORPONE.COM
   Name Server: NS3.MEGACORPONE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-10-13T23:25:05Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
```

Câu 5

Sử dụng whois để xem thử thông tin của uit.edu.vn

```
┌──(kali㉿kali)-[~]
└─$ 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 xem được vì TLD này không có whois server, do đó không thể trích xuất thông tin từ whois.

Câu 6:

Thu thập thông tin về tên miền uit.edu.vn

VNNIC INTERNET RESOURCE WHOIS INFORMATION

This whois query was received from IP Address: **42.119.112.74**
We recognize the resource in your query is: **Domain Name**
Type of domain name: **ASCII Domain Name**
Keyword in your query: **uit.edu.vn**

Domain information

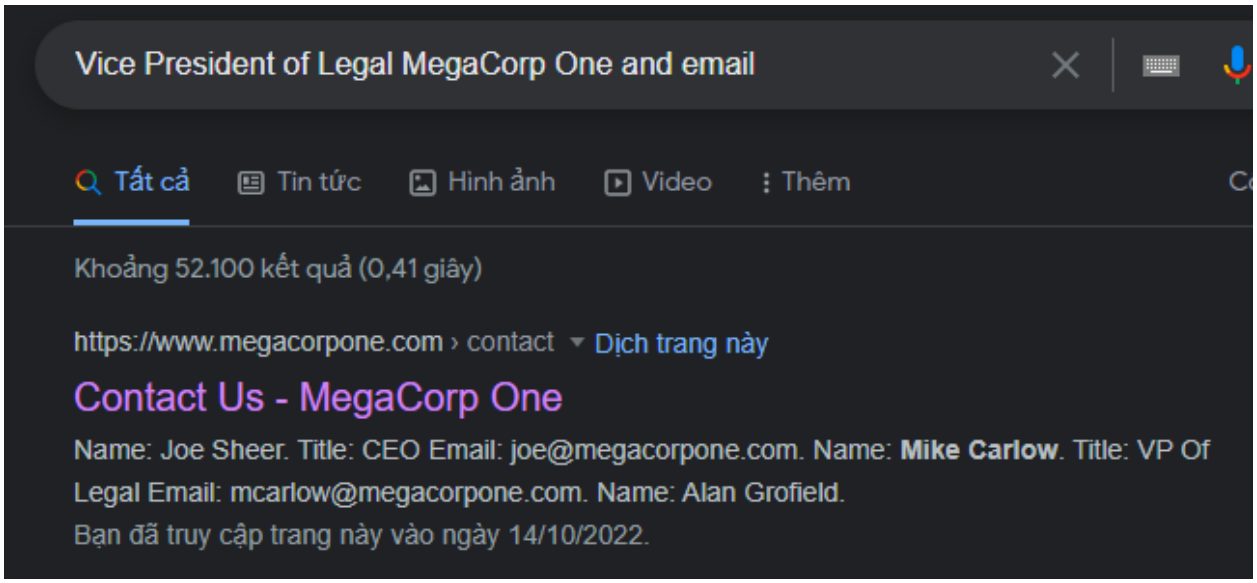
Domain Name:	uit.edu.vn
Registrant Name:	Trường Đại học Công nghệ Thông tin
Registrar:	Công ty TNHH PA Việt Nam
Creation Date:	2006-10-02
Expiration Date:	2023-10-02
Status:	clientTransferProhibited
Nameserver:	ns1.pavietnam.vn ns2.pavietnam.vn nsbak.pavietnam.net
DNSSEC:	unsigned

Keyword *

Domain name | IP Address | Vietnamese domain name

Câu 7:

Ta search Vice President of Legal MegaCorp One and email



Truy cập vào trang và kéo xuống cuối, ta được thông tin cần tìm:

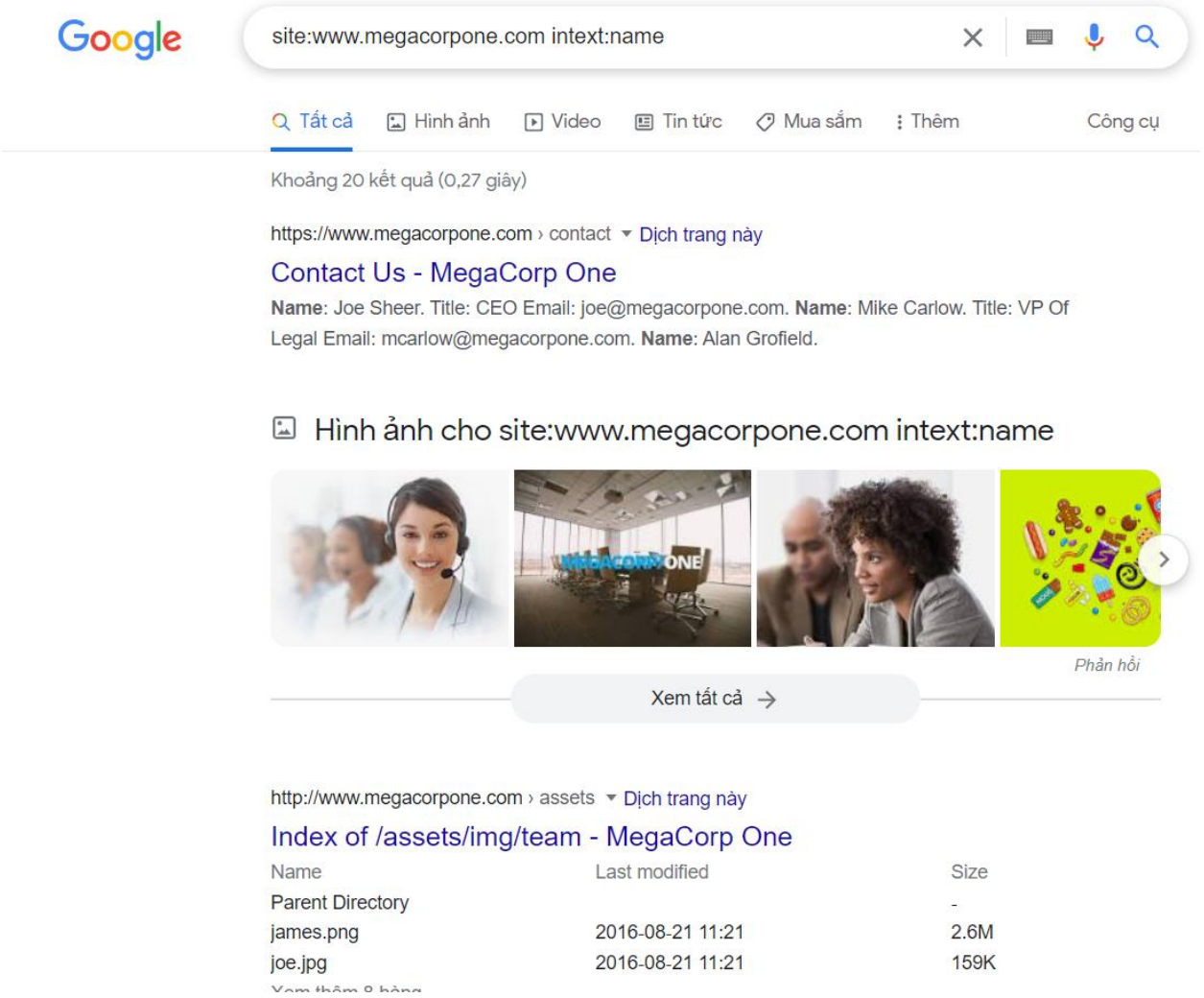
Name: Mike Carlow

Title: VP Of Legal
Email: mcarlow@megacorpone.com

Phó chủ tịch pháp lý của MegaCorp One là Mike Carlow, email là mcarlow@megacorpone.com

Câu 8:

Ta thấy được thêm được thông tin liên hệ, một số trang web đăng hình ảnh nhân viên khi sử dụng thêm "intext:name'



Câu 9:

Một vài từ khóa thường gặp trên google: filetype, inurl, intitle, site, index, intext, filetype

Câu 10:

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.

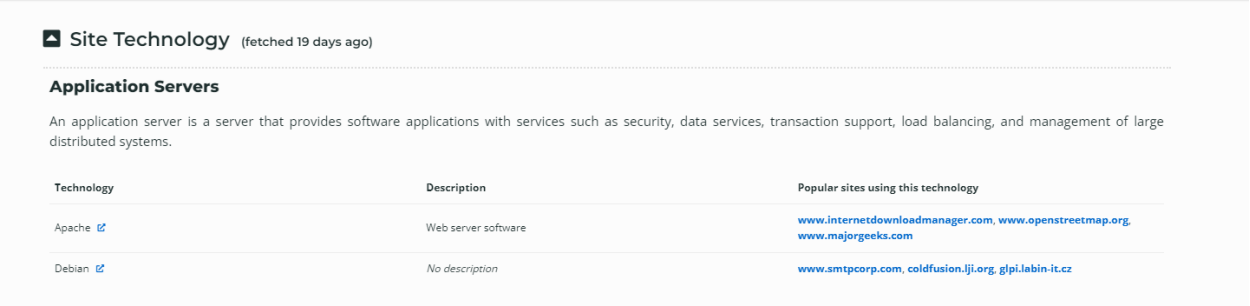
- Sinh viên không được gửi email vào group hoặc trả lời tất cả (reply all) email group này, tránh làm phiền các sinh viên khác.

- Nghiêm cấm dùng email group để phát tán quảng cáo, mời khảo sát.

Đây là thông tin có thể tìm kiếm trên google và dẫn link đến facebook. Không nên cung cấp thông tin này lên mạng vì có thể những thành phần xấu khi nắm được mail sinh viên có thể gửi mail fishing để lừa đảo nhấp vào link và thực hiện việc khai thác thông tin sinh viên.

Câu 11:

Máy chủ ứng dụng đang chạy trên www.megacorpone.com là



Site Technology (fetched 19 days ago)

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.internetdownloadmanager.com, www.openstreetmap.org, www.majorgeeks.com
Debian	*No description*	www.smtpcorp.com, coldfusion.lji.org, glpi.labin-it.cz

Câu 12:

Xuất hiện lỗi CAPTCHA triggered nên không thể thực hiện theo cách thông thường

Sử dụng netcraft

```
[recon-ng][default][netcraft] > run

MEGACORPONE.COM

[*] URL: http://searchdns.netcraft.com/?restriction=site%2Bends%2Bwith&host=megacorpone.com
[*] No results found.
[recon-ng][default][netcraft] >
```

Sử dụng google_site_web

```
[recon-ng][default][google_site_web] > run

MEGACORPONE.COM

[*] Searching Google for: site:megacorpone.com
[*] Country: None
[*] Host: www.megacorpone.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 201.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 301.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 401.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 501.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 601.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 701.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 801.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[!] Google CAPTCHA triggered. No bypass available.

SUMMARY

[*] 1 total (1 new) hosts found.
[recon-ng][default][google_site_web] >
```

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

+-------+---------------------+------------+--------+---------+----------+-----------+-------+----------------+
| rowid |        host         | ip_address | region | country | latitude | longitude | notes |     module     |
+-------+---------------------+------------+--------+---------+----------+-----------+-------+----------------+
| 1     | www.megacorpone.com |            |        |         |          |           |       | google_site_web |
+-------+---------------------+------------+--------+---------+----------+-----------+-------+----------------+

[*] 1 rows returned
[recon-ng][default] >
```

Ta có thể chạy resolve để check nhưng có một số vấn đề bên trên đề cập nên đã không thực hiện như thông thường được

```
[recon-ng][default][resolve] > run
[*] megacorpone.com ⇒ No answer
```

Câu 13:

Tương tự ở trang UIT cũng bị hạn chế do google CAPTCHA nên không thể thực hiện như thông thường

```
[recon-ng][default] > modules load recon/domains-hosts/google_site_web
[recon-ng][default][google_site_web] > options set SOURCE uit.edu.vn
SOURCE ⇒ uit.edu.vn
[recon-ng][default][google_site_web] > run
set SOURCE uit.edu.vn
----------
UIT.EDU.VN
----------
[*] Searching Google for: site:uit.edu.vn
[!] Google CAPTCHA triggered. No bypass available.
[recon-ng][default][google_site_web] > back
[recon-ng][default] > modules load recon/hosts-hosts/resolve
[recon-ng][default][resolve] > options set SOURCE uit.edu.vn
SOURCE ⇒ uit.edu.vn
[recon-ng][default][resolve] > run
[*] uit.edu.vn ⇒ 45.122.249.78
[recon-ng][default][resolve] >
```

Câu 14:

Ta sẽ thực hiện check code của thầy Vũ Tuấn Hải tại UIT

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ git clone https://github.com/vutuanhai237/FrontendStudyingBoard
Cloning into 'FrontendStudyingBoard' ...
remote: Enumerating objects: 5058, done.
remote: Counting objects: 100% (44/44), done.
remote: Compressing objects: 100% (34/34), done.
remote: Total 5058 (delta 33), reused 10 (delta 10), pack-reused 5014
Receiving objects: 100% (5058/5058), 6.55 MiB | 10.84 MiB/s, done.
Resolving deltas: 100% (3322/3322), done.

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

    gitleaks

6:51AM WRN leaks found: 1
6:51AM INF scan completed in 30.299876763s

┌──(kali㉿kali)-[~/Downloads]
└─$
```

Ta clone code từ github về và check với gitleaks với source từ nơi tải về và xuất báo cáo ra file json


```
[
 {
  "Description": "Generic API Key",
  "StartLine": 20,
  "EndLine": 20,
  "StartColumn": 26,
  "EndColumn": 82,
  "Match": "apiKey=\"pgsfnb617zvx79gf1fo6sauiik6bg2icroka7q4f1lelxesr\"",
  "Secret": "pgsfnb617zvx79gf1fo6sauiik6bg2icroka7q4f1lelxesr",
  "File": "src/component/layout/create_post.js",
  "Commit": "1a34ee322de8c67ce0569d661464d17690b14f3a",
  "Entropy": 4.4906015,
  "Author": "vutuanhai237",
  "Email": "43202025+vutuanhai237@users.noreply.github.com",
  "Date": "2020-04-28T15:30:13Z",
  "Message": "Merge branch 'master' of https://github.com/vutuanhai237/Front-end-bht.cnpm.uit.edu.vn\n\ncommit aef7a4860c0a6cb6f14a24b78527884a9f872256\nAuthor: vutuanhai237 \u003c43202025+vutuanh
  "Tags": [],
  "RuleID": "generic-api-key"
 }
]
```


Ta thấy có phát hiện 1 lỗi đó chính là Generic API Key

Câu 15:

Ta có thể kết hợp thêm các 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

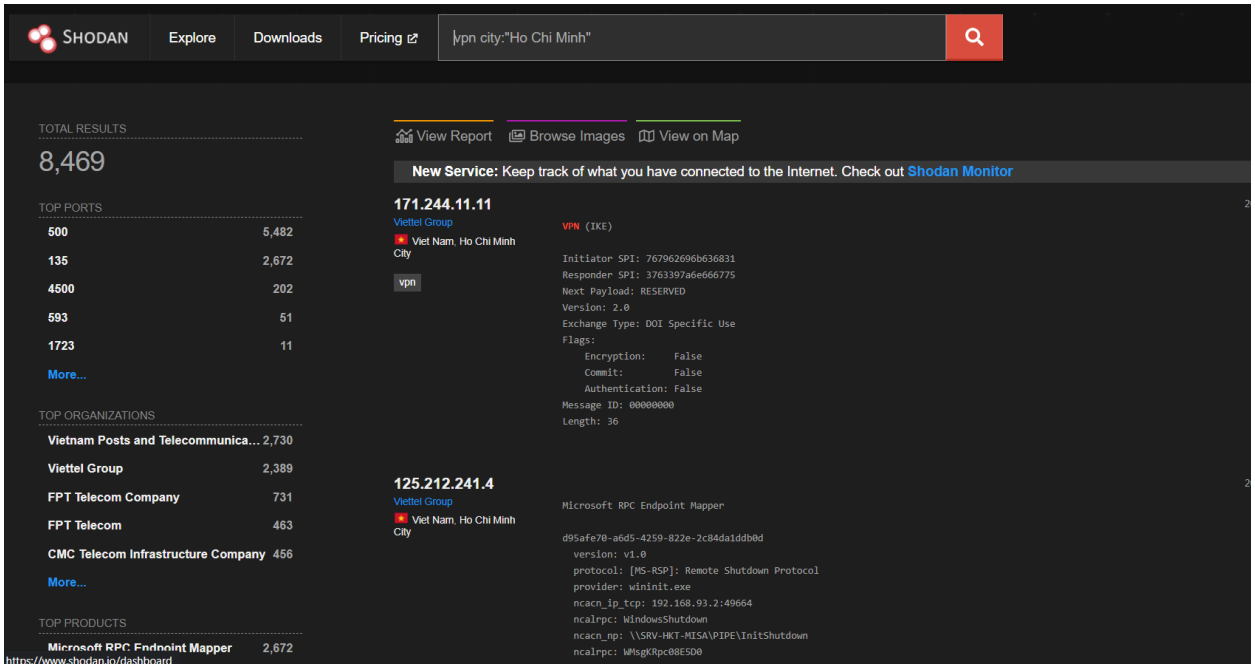
+: and vào 1 filter

-: or 1 filter

Before: trước thời gian nào đó

After: sau thời gian nào đó

Port: theo port



Câu 16:

	Shodan	Các công cụ tìm kiếm khác
Kết quả thông thường	Thông tin device (router, webcam, camera,...)	Thông tin content (url, file, text,...)

Service	Thông tin bị rò rỉ mà ta truy cập được	Thông tin liên quan đến dịch vụ (nhà cung cấp, ứng dụng hỗ trợ, doc hướng dẫn,...)
So với google Dorks	Tìm kiếm dịch vụ và thiết bị bị rò rỉ được hỗ trợ mặc định	Cần kết hợp từ khóa intitle, allintext,...

Câu 17:

Ở câu này ta sẽ thực hiện để check đường dẫn uit.edu.vn với baidu thì ta có được 3 kết quả email được tìm thấy

```
┌──(root㉿kali)-[~]
└─# theHarvester -d uit.edu.vn -b baidu

*******************************************************************
*                                                                 *
*  _   _                                            _             *
* | |_| |__    ___      /\  /\__ _ _ ____   _____ ___| |_ ___ _ __ *
* | __| '_ \ / _ \    / /_/ / _` | '__\ \ / / _ \ __| __/ _ \ '__|*
* | |_| | | |  __/   / __  / (_| | |   \ V /  __/\__ \ ||  __/ |   *
*  \__|_| |_|\___|   \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|   *
*                                                                 *
* theHarvester 4.0.3                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] Target: uit.edu.vn

[*] Searching Baidu.

[*] No IPs found.

[*] Emails found: 3
------------------
18521135@gm.uit.edu.vn
18521182@gm.uit.edu.vn
18521348@gm.uit.edu.vn

[*] Hosts found: 2
------------------
en.uit.edu.vn:192.168.20.23
gm.uit.edu.vn
```

Câu 18:

Tương tự với câu 17 ta sẽ thực hiện check đường dẫn với các công cụ khác nhau như Bing, Google, Baidu, Duckduckgo

Bing:

```
[*] Target: uit.edu.vn

        Searching 0 results.
[*] Searching Bing.

[*] No IPs found.

[*] Emails found: 3
------------------
inseclab@uit.edu.vn
mapr@uit.edu.vn
vund@uit.edu.vn

[*] Hosts found: 33
-------------------
cnsc.uit.edu.vn:192.168.77.252
courses.uit.edu.vn:192.168.20.64
ctsv.uit.edu.vn:192.168.20.98
daa.uit.edu.vn:192.168.20.47
dkhp.uit.edu.vn:192.168.20.233
drl.uit.edu.vn:192.168.20.98
en.uit.edu.vn:192.168.20.23
fce.uit.edu.vn:192.168.20.38
fit.uit.edu.vn:192.168.20.60
forum.uit.edu.vn:192.168.20.29
httt.uit.edu.vn:192.168.20.43
inseclab.uit.edu.vn:10.101.0.2
iot.uit.edu.vn:192.168.20.218
jobs.uit.edu.vn:192.168.20.211
khcn.uit.edu.vn:192.168.20.114
khmt.uit.edu.vn:192.168.20.46
khtc.uit.edu.vn:192.168.20.23
mapr.uit.edu.vn:192.168.20.98
nc.uit.edu.vn:192.168.20.232
nlp.uit.edu.vn:10.71.13.119
oep.uit.edu.vn:192.168.20.47
portal.uit.edu.vn:192.168.20.88
qhdn.uit.edu.vn:192.168.20.114
se.uit.edu.vn:192.168.20.56
student.uit.edu.vn:192.168.20.47
thuvien.uit.edu.vn:192.168.20.126
tuoitre.uit.edu.vn:192.168.20.160
tuyensinh.uit.edu.vn:192.168.20.23
ucpc.uit.edu.vn:192.168.20.112
www.uit.edu.vn:192.168.20.23
```

Google:

```
[*] Target: uit.edu.vn

        Searching 0 results.
        Searching 100 results.
        Searching 200 results.
        Searching 300 results.
        Searching 400 results.
        Searching 500 results.
[*] Searching Google.

[*] No IPs found.

[*] Emails found: 11
----------------------
14521097@gm.uit.edu.vn
14521108@gm.uit.edu.vn
cfl@uit.edu.vn
info@uit.edu.vn
mssv@ms.uit.edu.vn
ngoclv@uit.edu.vn
quanlt@uit.edu.vn
thindv@uit.edu.vn
tuyensinh@uit.edu.vn
x22lungvd@uit.edu.vn
x22ngoclv@uit.edu.vn

[*] Hosts found: 27
---------------------
chungthuc.uit.edu.vn:192.168.20.22
course.uit.edu.vn:192.168.20.64
courses.uit.edu.vn:192.168.20.64
cs.uit.edu.vn:192.168.20.46
ctsv.uit.edu.vn:192.168.20.98
daa.uit.edu.vn:192.168.20.47
en.uit.edu.vn:192.168.20.23
gm.uit.edu.vn
huongnghiep.uit.edu.vn:192.168.20.47
i-english.uit.edu.vn:192.168.20.175
mail.gm.uit.edu.vn:142.250.207.83
ms.uit.edu.vn
qldt.uit.edu.vn:192.168.20.69
student.uit.edu.vn:192.168.20.47
thuvien.uit.edu.vn:192.168.20.126
tttdtt.uit.edu.vn:192.168.20.108
tuyensinh.uit.edu.vn:192.168.20.23
www.uit.edu.vn:192.168.20.23
x22courses.uit.edu.vn
x22cs.uit.edu.vn
x22huongnghiep.uit.edu.vn
```

Baidu:

```
┌──(root㉿kali)-[~]
└─# theHarvester -d uit.edu.vn -b baidu

*******************************************************************
*                                                                 *
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.0.3                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] Target: uit.edu.vn

[*] Searching Baidu.

[*] No IPs found.

[*] Emails found: 3
____________________
18521135@gm.uit.edu.vn
18521182@gm.uit.edu.vn
18521348@gm.uit.edu.vn

[*] Hosts found: 2
____________________
en.uit.edu.vn:192.168.20.23
gm.uit.edu.vn
```

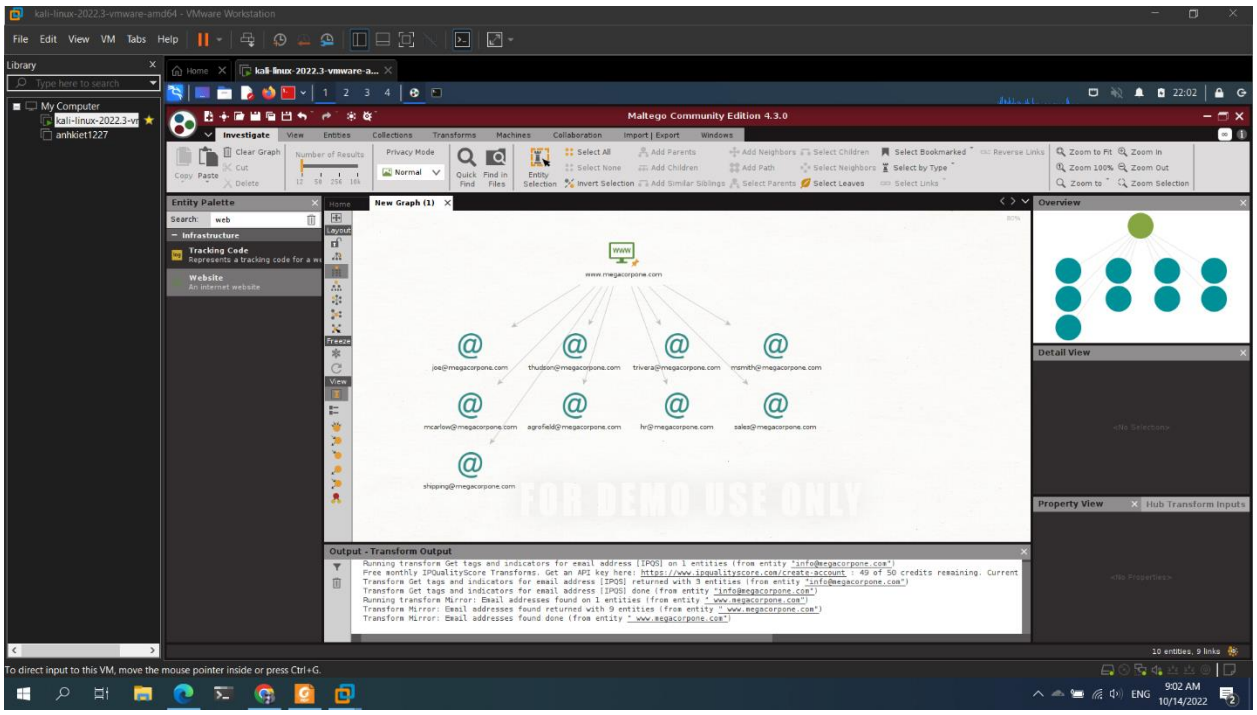
Duckduckgo:

```
[*] Target: uit.edu.vn

[*] Searching Duckduckgo.

[*] No IPs found.

[*] Emails found: 1
------------------
info@uit.edu.vn

[*] Hosts found: 34
-------------------
auth.uit.edu.vn:192.168.20.22
banqlcs.uit.edu.vn:192.168.20.47
cd.uit.edu.vn:192.168.20.84
chungthuc.uit.edu.vn:192.168.20.22
cnsc.uit.edu.vn:192.168.77.252
courses.uit.edu.vn:192.168.20.64
cs.uit.edu.vn:192.168.20.46
ctgt.uit.edu.vn:192.168.20.62
ctsv.uit.edu.vn:192.168.20.98
dangbo.uit.edu.vn:192.168.20.62
dbcl.uit.edu.vn:192.168.20.84
dreamspark.uit.edu.vn:192.168.20.8
en.uit.edu.vn:192.168.20.23
fce.uit.edu.vn:192.168.20.38
fit.uit.edu.vn:192.168.20.60
forum.uit.edu.vn:192.168.20.29
httt.uit.edu.vn:192.168.20.43
khcn.uit.edu.vn:192.168.20.114
khtc.uit.edu.vn:192.168.20.23
mail.gm.uit.edu.vn:142.250.207.83
mail.uit.edu.vn:142.250.207.83
nc.uit.edu.vn:192.168.20.232
oep.uit.edu.vn:192.168.20.47
phongdl.uit.edu.vn:192.168.20.84
portal.uit.edu.vn:192.168.20.88
qttb.uit.edu.vn:192.168.20.84
sdh.uit.edu.vn:192.168.20.23
se.uit.edu.vn:192.168.20.56
student.uit.edu.vn:192.168.20.47
tchc.uit.edu.vn:192.168.20.84
thuvien.uit.edu.vn:192.168.20.126
tuoitre.uit.edu.vn:192.168.20.160
tuyensinh.uit.edu.vn:192.168.20.23
www.uit.edu.vn:192.168.20.23
```

Có thể thấy duckduckgo get được nhiều host nhất và google get được nhiều email nhất

Câu 19:

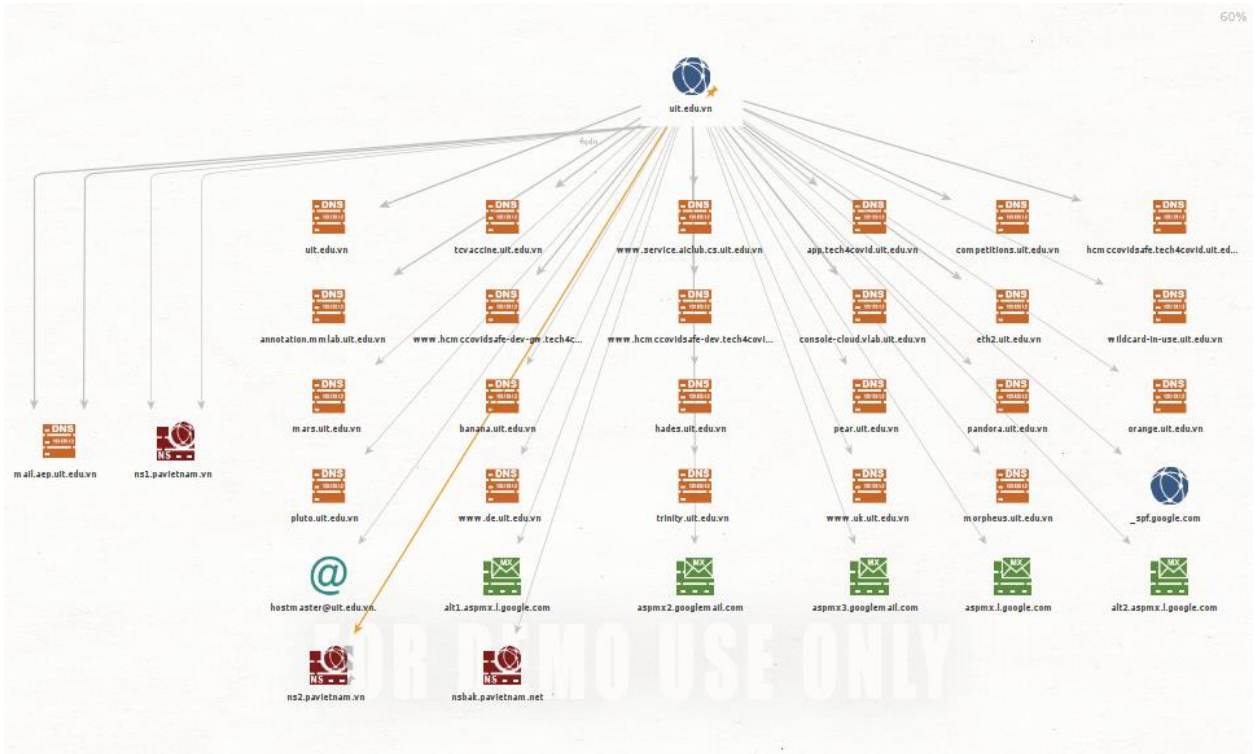
Ta sẽ add thêm đường dẫn vào máy tính và sau đó mở thêm các mục để xem email



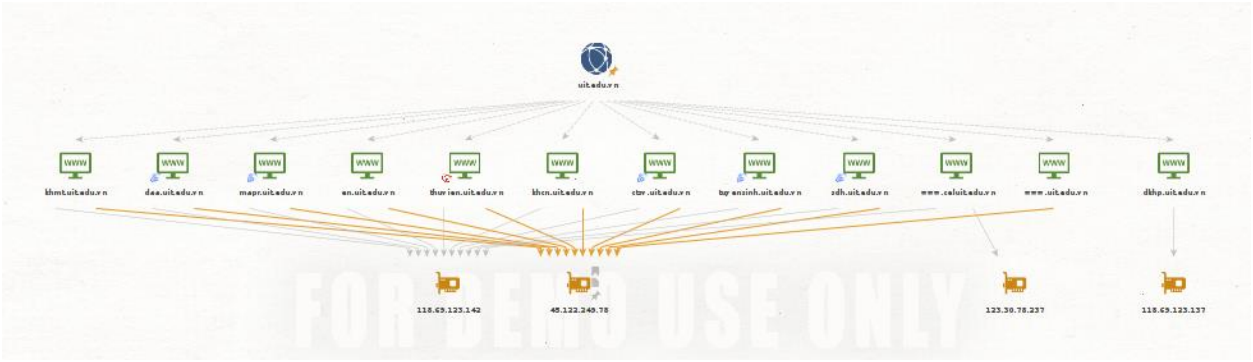
Câu 20:

Câu a:

Tương tự ta sẽ add đường dẫn và mở thêm các dns để có thể xem được



Câu b: ở phần này ta sẽ xem các tên miền liên quan đến uit.edu.vn và từ đó check từ các tên mình để có thể xem



Câu 21:

Có thể thấy có SOA, SRV, AFSDB, DCHID, HIP

Link tham khảo: https://www.cloudflare.com/learning/dns/dns-records/

What are the most common types of DNS record?

- **A record** - The record that holds the IP address of a domain. Learn more about the A record.
- **AAAA record** - The record that contains the IPv6 address for a domain (as opposed to A records, which list the IPv4 address). Learn more about the AAAA record.
- **CNAME record** - Forwards one domain or subdomain to another domain, does NOT provide an IP address. Learn more about the CNAME record.
- **MX record** - Directs mail to an email server. Learn more about the MX record.
- **TXT record** - Lets an admin store text notes in the record. These records are often used for email security. Learn more about the TXT record.
- **NS record** - Stores the name server for a DNS entry. Learn more about the NS record.
- **SOA record** - Stores admin information about a domain. Learn more about the SOA record.
- **SRV record** - Specifies a port for specific services. Learn more about the SRV record.
- **PTR record** - Provides a domain name in reverse-lookups. Learn more about the PTR record.

Câu 22:

```
┌──(root㉿kali)-[~]
└─# host -t txt uit.edu.vn
uit.edu.vn has no TXT record

┌──(root㉿kali)-[~]
└─# host -t mx uit.edu.vn
uit.edu.vn mail is handled by 10 aspmx.l.google.com.
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 40 aspmx3.googlemail.com.

┌──(root㉿kali)-[~]
└─#
```

Câu 23:

```
┌──(kali㉿kali)-[~]
└─$ host idontexist.uit.edu.vn
idontexist.uit.edu.vn has address 45.122.249.78
idontexist.uit.edu.vn has address 118.69.123.142

┌──(kali㉿kali)-[~]
└─$ host noexist.uit.edu.vn
noexist.uit.edu.vn has address 118.69.123.142
noexist.uit.edu.vn has address 45.122.249.78

┌──(kali㉿kali)-[~]
└─$ host baithuchanhso2.uit.edu.vn
baithuchanhso2.uit.edu.vn has address 118.69.123.142
baithuchanhso2.uit.edu.vn has address 45.122.249.78
```

Các địa chỉ IP đều giống nhau vì cấu hình DNS của tên miền uit.edu.vn có sử dụng wildcard * nên nếu xảy ra trường hợp 1 DNS query nào đó không có hostname thì sẽ được match với wildcard * trả về cùng 1 IP

Câu 24:

Wordlist:
https://github.com/danielmiessler/SecLists/blob/285474cf9bff85f3323c5a1ae436f78acd1cb62c/Discovery/DNS/subdomains-top1million-5000.txt

```
┌──(root㉿kali)-[~]
└─# for name in $(cat /home/kali/Downloads/namelist.txt ); do host $name.megacorpone.com; done | grep -v "not foun
d"~
www.megacorpone.com has address 149.56.244.87
mail.megacorpone.com has address 51.222.169.212
ftp.megacorpone.com has address 125.235.4.59
localhost.megacorpone.com has address 125.235.4.59
webmail.megacorpone.com has address 125.235.4.59
smtp.megacorpone.com has address 125.235.4.59
webdisk.megacorpone.com has address 125.235.4.59
pop.megacorpone.com has address 125.235.4.59
cpanel.megacorpone.com has address 125.235.4.59
whm.megacorpone.com has address 125.235.4.59
ns1.megacorpone.com has address 51.79.37.18
ns2.megacorpone.com has address 51.222.39.63
autodiscover.megacorpone.com has address 125.235.4.59
autoconfig.megacorpone.com has address 125.235.4.59
ns.megacorpone.com has address 125.235.4.59
test.megacorpone.com has address 51.222.169.219
m.megacorpone.com has address 125.235.4.59
blog.megacorpone.com has address 125.235.4.59
dev.megacorpone.com has address 125.235.4.59
www2.megacorpone.com has address 149.56.244.87
ns3.megacorpone.com has address 66.70.207.180
pop3.megacorpone.com has address 125.235.4.59
forum.megacorpone.com has address 125.235.4.59
admin.megacorpone.com has address 51.222.169.208
mail2.megacorpone.com has address 51.222.169.213
vpn.megacorpone.com has address 51.222.169.220
mx.megacorpone.com has address 125.235.4.59
imap.megacorpone.com has address 125.235.4.59
old.megacorpone.com has address 125.235.4.59
new.megacorpone.com has address 125.235.4.59
mobile.megacorpone.com has address 125.235.4.59
mysql.megacorpone.com has address 125.235.4.59
beta.megacorpone.com has address 51.222.169.209
support.megacorpone.com has address 51.222.169.218
cp.megacorpone.com has address 125.235.4.59
```

Câu 25:

Code

```
#! /bin/bash
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")

for domain in ${domains[@]}; do
        echo "Print the domain: $domain"
        for nameServer in `host -t ns $domain 2> /dev/null | cut -d " " -f 4`; do
                echo "Print the nameserver: $nameServer"
                echo "Print the zone transfer"
                host -l $domain $nameServer 2> /dev/null
                echo
                echo "-----------------------###This is the end of 1 domain of shool###--------------------------------"
        done
        echo
        echo "########################---This is the end of 1 school domain---###################################"
        echo
done
```

Kết quả:

Print the domain: hcmus.edu.vn

Print the nameserver: found:

Print the zone transfer

-----------------------###This is the end of 1 domain of shool###-----------------------------
---

##########---This is the end of 1 school domain---
##########

Print the domain: hcmussh.edu.vn

Print the nameserver: server.vnuhcm.edu.vn.

Print the zone transfer

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.

----------###This is the end of 1 domain of shool###----------
---

Print the nameserver: vnuserv.vnuhcm.edu.vn.

Print the zone transfer

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.

----------###This is the end of 1 domain of shool###----------
---

##########---This is the end of 1 school domain---
##########

Print the domain: uit.edu.vn
Print the nameserver: ns1.pavietnam.vn.
Print the zone transfer
Using domain server:
Name: ns1.pavietnam.vn.
Address: 112.213.89.3#53
Aliases:

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

----------###This is the end of 1 domain of shool###----------
---
Print the nameserver: ns2.pavietnam.vn.
Print the zone transfer
Using domain server:
Name: ns2.pavietnam.vn.
Address: 222.255.121.247#53
Aliases:

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

----------###This is the end of 1 domain of shool###----------
---
Print the nameserver: nsbak.pavietnam.net.
Print the zone transfer
Using domain server:
Name: nsbak.pavietnam.net.
Address: 112.213.89.22#53
Aliases:

Host uit.edu.vn not found: 5(REFUSED)

; Transfer failed.

----------###This is the end of 1 domain of shool###----------
---

##########---This is the end of 1 school domain---
##########

Print the domain: hcmut.edu.vn

Print the nameserver: dns3.hcmut.edu.vn.

Print the zone transfer

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.

----------###This is the end of 1 domain of shool###----------
---

Print the nameserver: dns1.hcmut.edu.vn.

Print the zone transfer

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.

----------###This is the end of 1 domain of shool###----------
---

Print the nameserver: dns2.hcmut.edu.vn.
Print the zone transfer
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.

----------###This is the end of 1 domain of shool###----------
---
Print the nameserver: dns4.hcmut.edu.vn.
Print the zone transfer
Using domain server:
Name: dns4.hcmut.edu.vn.
Address: 203.205.32.236#53
Aliases:

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

----------###This is the end of 1 domain of shool###----------
---

##########---This is the end of 1 school domain---
##########

Print the domain: hcmiu.edu.vn
Print the nameserver: hcm-server1.vnn.vn.
Print the zone transfer
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.

----------###This is the end of 1 domain of shool###----------
---
Print the nameserver: vdc-hn01.vnn.vn.
Print the zone transfer
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.

----------###This is the end of 1 domain of shool###----------
---

##########---This is the end of 1 school domain---
##########

Print the domain: uel.edu.vn
Print the nameserver: ns2.dns.net.vn.
Print the zone transfer
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.

----------###This is the end of 1 domain of shool###----------
---

Print the nameserver: ns1.dns.net.vn.

Print the zone transfer

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.

----------###This is the end of 1 domain of shool###----------
---

##########---This is the end of 1 school domain---
##########

Print the domain: hcmier.edu.vn

Print the nameserver: vnuserv.vnuhcm.edu.vn.

Print the zone transfer

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.

----------###This is the end of 1 domain of shool###----------
---

Print the nameserver: server.vnuhcm.edu.vn.

Print the zone transfer

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.

----------###This is the end of 1 domain of shool###----------

##########---This is the end of 1 school domain---
##########

Print the domain: vnuhcm.edu.vn

Print the nameserver: vnuserv.vnuhcm.edu.vn.

Print the zone transfer

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.

----------###This is the end of 1 domain of shool###----------

Print the nameserver: ns2.vdc2.vn.

Print the zone transfer

Using domain server:

Name: ns2.vdc2.vn.

Address: 14.225.232.23#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
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
kskнsvtn.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 10.159.136.186
ns1.vnuhcm.edu.vn has address 10.159.136.186
ns2.vnuhcm.edu.vn has address 10.159.136.186
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 10.159.136.186
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 10.159.136.186
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

----------###This is the end of 1 domain of shool###----------
---

Print the nameserver: ns1.vdc2.vn.

Print the zone transfer
Using domain server:
Name: ns1.vdc2.vn.
Address: 14.225.232.186#53
Aliases:

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

----------###This is the end of 1 domain of shool###----------
---
Print the nameserver: server.vnuhcm.edu.vn.
Print the zone transfer
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.

----------###This is the end of 1 domain of shool###----------
---

##########---This is the end of 1 school domain---
##

Câu 26:
Tham khảo: https://manpages.ubuntu.com/manpages/bionic/man1/dnsrecon.1.html
Ta sẽ có danh sách sau;
Specify the type of enumeration to perform (comma separated):
std To Enumerate general record types, enumerates.
SOA, NS, A, AAAA, MX and SRV if AXRF on the

NS Servers fail.

rvl To Reverse Look Up a given CIDR IP range.

brt To Brute force Domains and Hosts using a given dictionary.

srv To Enumerate common SRV Records for a given domain.

axfr Test all NS Servers in a domain for misconfigured zone transfers.

goo Perform Google search for sub-domains and hosts.

bing Perform Bing search for sub-domains and hosts.

snoop To Perform a Cache Snooping against all NS servers for a given domain, testing all with file containing the domains, file given with -D option.

tld Will remove the TLD of given domain and test against all TLD's registered in IANA

```
Specify the type of enumeration to perform (comma separated):
       std      To Enumerate general record types, enumerates.
                SOA, NS, A, AAAA, MX and SRV if AXRF on the
                NS Servers fail.
       rvl      To Reverse Look Up a given CIDR IP range.

       brt      To Brute force Domains and Hosts using a given
                dictionary.

       srv      To Enumerate common SRV Records for a given
                domain.

       axfr     Test all NS Servers in a domain for misconfigured
                   zone transfers.

       goo      Perform Google search for sub-domains and hosts.

       bing     Perform Bing search for sub-domains and hosts.

       snoop    To Perform a Cache Snooping against all NS
                servers for a given domain, testing all with
                file containing the domains, file given with -D
                option.

       tld      Will remove the TLD of given domain and test against
                all TLD's registered in IANA
```

Câu 27:

Ta sẽ kết hợp thêm thread trong công cụ dnsrecon

```
┌──(kali㉿kali)-[~/Downloads/lab2antoanmang]
└─$ dnsrecon -d megacorpone.com -D /home/kali/Downloads/lab2antoanmang/namelist2.txt -t brt --threads 4
[*] Using the dictionary file: /home/kali/Downloads/lab2antoanmang/namelist2.txt (provided by user)
[*] brt: Performing host and subdomain brute force against megacorpone.com...
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to 125.235.4.59
[!] All queries will resolve to this list of addresses!!
[*] Do you wish to continue? [Y/n]
y
[+]     A ftp.megacorpone.com 125.235.4.59
[+]     A localhost.megacorpone.com 125.235.4.59
[+]     A mail.megacorpone.com 51.222.169.212
[+]     A www.megacorpone.com 149.56.244.87
[+]     A smtp.megacorpone.com 125.235.4.59
[+]     A webmail.megacorpone.com 125.235.4.59
[+]     A pop.megacorpone.com 125.235.4.59
[+]     A webdisk.megacorpone.com 125.235.4.59
[+]     A cpanel.megacorpone.com 125.235.4.59
[+]     A whm.megacorpone.com 125.235.4.59
[+]     A ns1.megacorpone.com 51.79.37.18
[+]     A ns2.megacorpone.com 51.222.39.63
[+]     A autoconfig.megacorpone.com 125.235.4.59
[+]     A test.megacorpone.com 51.222.169.219
[+]     A autodiscover.megacorpone.com 125.235.4.59
[+]     A ns.megacorpone.com 125.235.4.59
[+]     A m.megacorpone.com 125.235.4.59
[+]     A dev.megacorpone.com 125.235.4.59
[+]     A blog.megacorpone.com 125.235.4.59
[+]     A www2.megacorpone.com 149.56.244.87
[+]     A ns3.megacorpone.com 66.70.207.180
[+]     A forum.megacorpone.com 125.235.4.59
[+]     A pop3.megacorpone.com 125.235.4.59
[+]     A admin.megacorpone.com 51.222.169.208
[+]     A mail2.megacorpone.com 51.222.169.213
[+]     A imap.megacorpone.com 125.235.4.59
[+]     A old.megacorpone.com 125.235.4.59
[+]     A new.megacorpone.com 125.235.4.59
[+]     A mobile.megacorpone.com 125.235.4.59
[+]     A mysql.megacorpone.com 125.235.4.59
[+]     A beta.megacorpone.com 51.222.169.209
[+]     A support.megacorpone.com 51.222.169.218
[+]     A mx.megacorpone.com 125.235.4.59
[+]     A vpn.megacorpone.com 51.222.169.220
[+]     A cp.megacorpone.com 125.235.4.59
[+]     A secure.megacorpone.com 125.235.4.59
[+]     A shop.megacorpone.com 125.235.4.59
[+]     A demo.megacorpone.com 125.235.4.59
[+]     A dns2.megacorpone.com 125.235.4.59
[+]     A ns4.megacorpone.com 125.235.4.59
[+]     A static.megacorpone.com 125.235.4.59
[+]     A dns1.megacorpone.com 125.235.4.59
[+]     A lists.megacorpone.com 125.235.4.59
[+]     A web.megacorpone.com 125.235.4.59
[+]     A www1.megacorpone.com 125.235.4.59
[+]     A img.megacorpone.com 125.235.4.59
[+]     A portal.megacorpone.com 125.235.4.59
[+]     A server.megacorpone.com 125.235.4.59
[+]     A wiki.megacorpone.com 125.235.4.59
[+] 49 Records Found

┌──(kali㉿kali)-[~/Downloads/lab2antoanmang]
└─$
```

Câu 28:

Kết hợp thêm tùy chọn tcp trong công cụ dnsrecon

```
┌──(kali㉿kali)-[~/Downloads/lab2antoanmang]
└─$ dnsrecon -d megacorpone.com --tcp
[*] std: Performing General Enumeration against: megacorpone.com...
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to 125.235.4.59
[!] All queries will resolve to this list of addresses!!
[-] DNSSEC is not configured for megacorpone.com
[*]      SOA ns1.megacorpone.com 51.79.37.18
[*]      NS ns3.megacorpone.com 66.70.207.180
[*]      NS ns2.megacorpone.com 51.222.39.63
[*]      NS ns1.megacorpone.com 51.79.37.18
[*]      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 217.70.178.1
[*]      MX mail.megacorpone.com 51.222.169.212
[*]      TXT megacorpone.com Try Harder
[*]      TXT megacorpone.com google-site-verification=U7B_b0HNeBtY4qYGQZNsEYXfCJ32hMNV3GtC0wWq5pA
[*] Enumerating SRV Records
[+] 0 Records Found
```

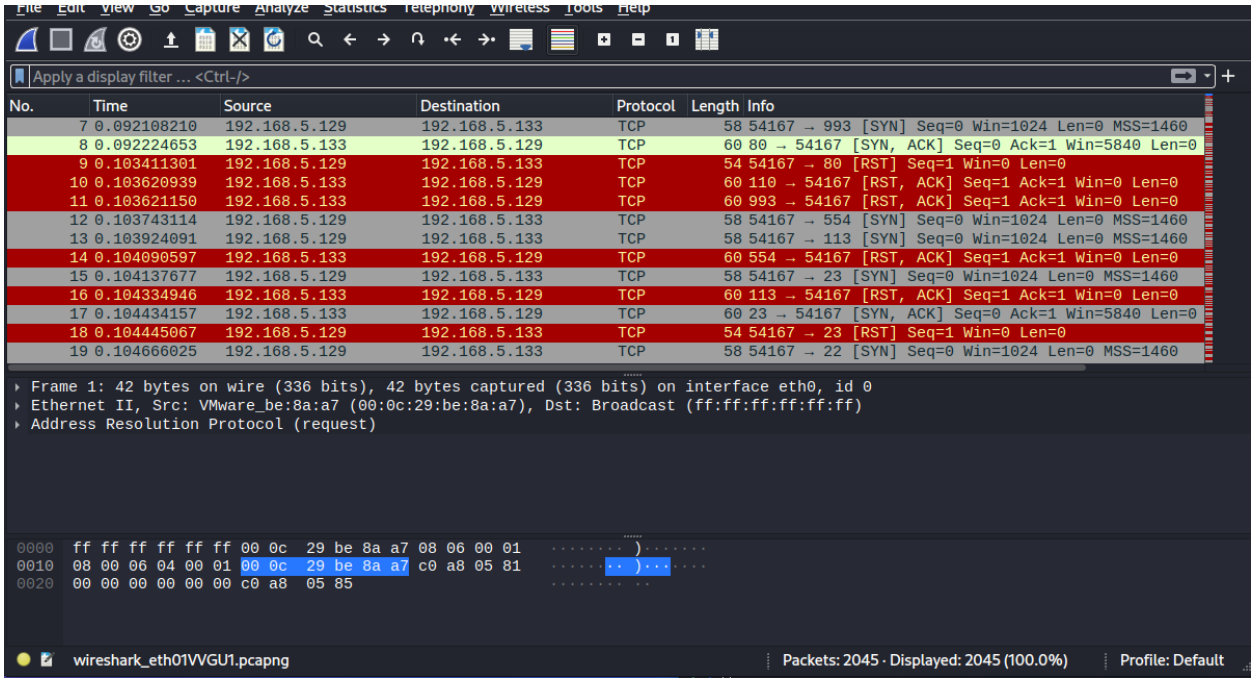
Câu 29:

Dùng “nmap -sS” để thực hiện TCP SYN scan.

Ta quét máy Metasploitable có địa chỉ 192.168.5.133

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.5.133
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-20 04:11 EDT
Nmap scan report for 192.168.5.133
Host is up (0.0017s 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:29:18:B6:48 (VMware)

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

Wireshark:

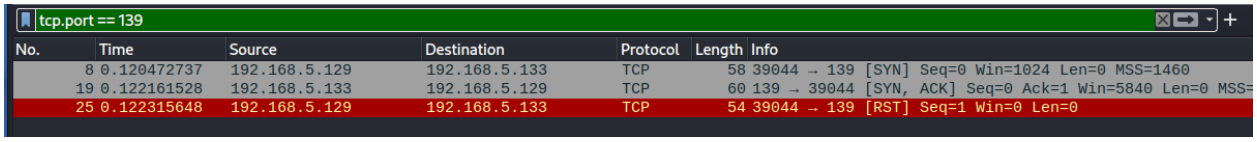


Tại port 139 đang mở (kết quả quét từ lệnh nmap) :

Ở gói 8, ta có thể thấy máy ta (192.168.5.129) gởi gói SYN tới máy 192.168.5.133

Ở gói 19, ta có thể thấy máy 192.168.5.133 gởi lại gói SYN, ACK tới máy 192.168.5.129 để hoàn thành quá trình bắt tay ba bước

Ở gói 25, ta có thể thấy máy ta (192.168.5.129) gởi gói RST tới máy 192.168.5.113 để kết thúc kết nối

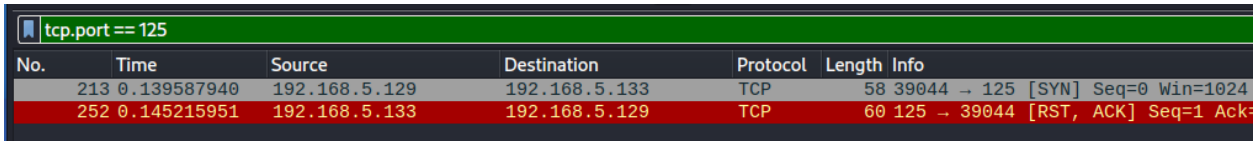


Tại port 125:

Ở gói 213, ta có thể thấy máy ta (192.168.5.129) gởi gói SYN tới máy 192.168.5.133

Ở gói 252, ta có thể thấy máy 192.168.5.133 gởi gói RST, ACK tới máy 192.168.5.129

=> prot 125 đang đóng



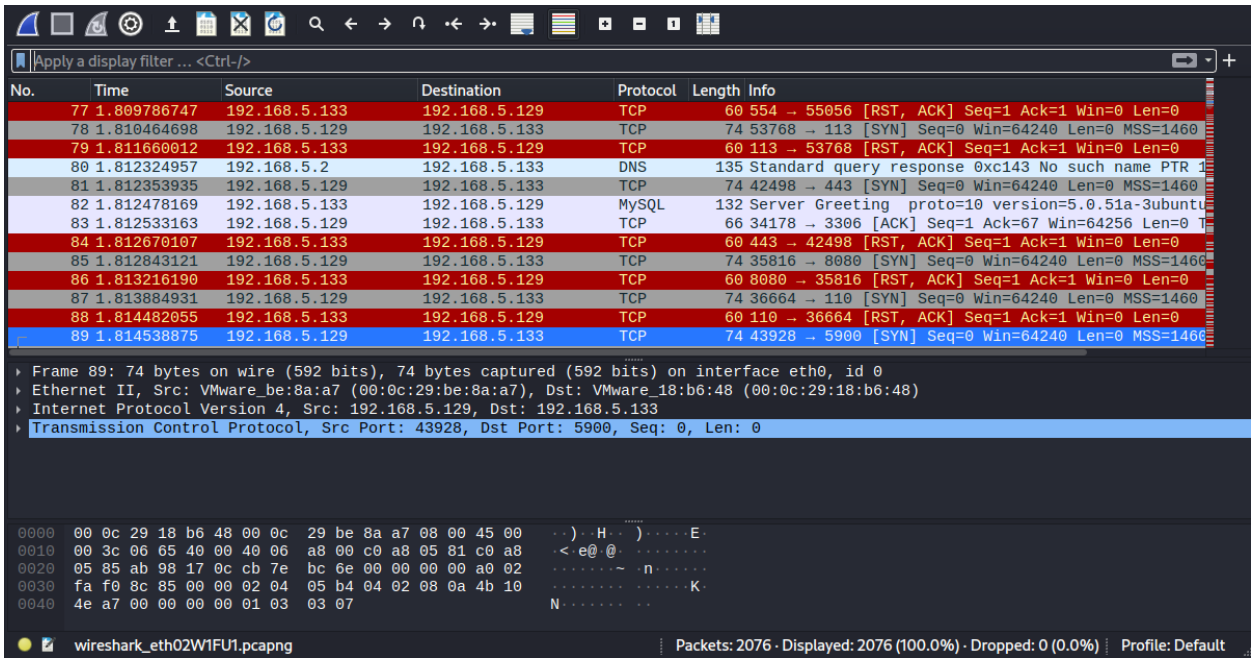
Câu 30:

Dùng “nmap -sT” để thực hiện TCP connect scan.

Ta quét máy Metasploitable có địa chỉ 192.168.5.133

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.5.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-20 05:48 EDT
Nmap scan report for 192.168.5.133
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

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
```

Khi bật wireshark trong quá trình chạy nmap, ta bắt lấy rất nhiều gói tin



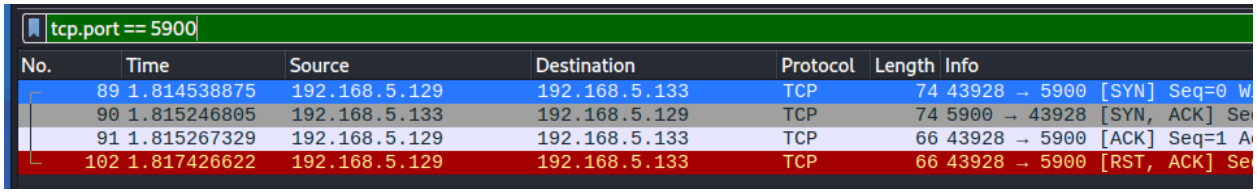
Từ kết quả sau khi chạy nmap, ta thử kiểm tra lại xem port 5900 có đang mở không:

Ở gói 89, máy ta gửi gói SYN tới 192.168.5.133.

Ở gói 90, máy 192.168.5.133 gửi gói SYN/ACK tới lại máy ta.

Ở gói 91 và 102, máy ta phản hồi lại gói ACK và gói RST, ACK cho máy 192.168.5.133

Kết luận: port 5900 đang mở.



Câu 31: So sánh khi dùng TCP connect scan và SYN Scan:

Phương thức quét	TCP connect scan	SYN Scan
Số lượng gói tin được gửi	1054	1023
Số lượng gói tin được nhận	1006	1000
Thời gian quét	0,26s	0,61s

Câu 32:

Code python:

```
import os

IP = input("[+] Enter the Host IP Address:\t")
print("[+] Starting Ping Sweeper on " + IP)
dot = IP.rfind(".")
IP = IP[0:dot + 1]

for i in range(1, 255):
    host = IP + str(i)
    response = os.system("ping -c 1 -w 1 " + host + " >/dev/null")

    if response == 0:
        print(host + " is up")
```

```
┌──(kali㉿kali)-[~/UIT/NT101]
└─$ python3 bai32_hostScanner.py
[+] Enter the Host IP Address:  192.168.5.1
[+] Starting Ping Sweeper on 192.168.5.1
192.168.5.1 is up
192.168.5.2 is up
192.168.5.129 is up
192.168.5.133 is up
```

Từ kết quả trên, ta thấy được có 4 host đang hoạt động trong mạng.

Câu 33:

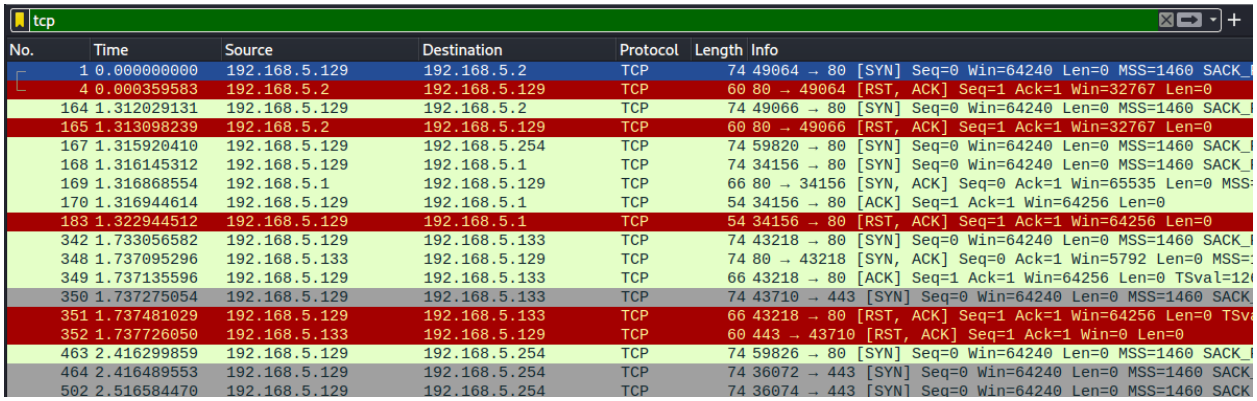
```
┌──(kali㉿kali)-[~/UIT/NT101]
└─$ nmap -v -sn 192.168.5.1-254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-20 07:11 EDT
Initiating Ping Scan at 07:11
Scanning 254 hosts [2 ports/host]
Completed Ping Scan at 07:11, 2.94s elapsed (254 total hosts)
Initiating Parallel DNS resolution of 4 hosts. at 07:11
Completed Parallel DNS resolution of 4 hosts. at 07:11, 0.01s elapsed
Nmap scan report for 192.168.5.1
Host is up (0.0068s latency).
Nmap scan report for 192.168.5.2
Host is up (0.0014s latency).
Nmap scan report for 192.168.5.3 [host down]
Nmap scan report for 192.168.5.4 [host down]
Nmap scan report for 192.168.5.5 [host down]
Nmap scan report for 192.168.5.6 [host down]
Nmap scan report for 192.168.5.7 [host down]
Nmap scan report for 192.168.5.8 [host down]
Nmap scan report for 192.168.5.9 [host down]
Nmap scan report for 192.168.5.10 [host down]
Nmap scan report for 192.168.5.11 [host down]
Nmap scan report for 192.168.5.12 [host down]
Nmap scan report for 192.168.5.13 [host down]
Nmap scan report for 192.168.5.14 [host down]
Nmap scan report for 192.168.5.15 [host down]
Nmap scan report for 192.168.5.16 [host down]
Nmap scan report for 192.168.5.17 [host down]
Nmap scan report for 192.168.5.18 [host down]
Nmap scan report for 192.168.5.19 [host down]
Nmap scan report for 192.168.5.20 [host down]
Nmap scan report for 192.168.5.21 [host down]
Nmap scan report for 192.168.5.22 [host down]
Nmap scan report for 192.168.5.23 [host down]
```

Wireshark:

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.5.129	192.168.5.2	TCP	74	49064 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2	0.000127345	VMware_be:8a:a7	Broadcast	ARP	42	Who has 192.168.5.3? Tell 192.168.5.129
3	0.000272966	VMware_be:8a:a7	Broadcast	ARP	42	Who has 192.168.5.4? Tell 192.168.5.129
4	0.000359583	192.168.5.2	192.168.5.129	TCP	60	80 → 49064 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=
5	0.000389748	VMware_be:8a:a7	Broadcast	ARP	42	Who has 192.168.5.5? Tell 192.168.5.129
6	0.000542010	VMware_be:8a:a7	Broadcast	ARP	42	Who has 192.168.5.6? Tell 192.168.5.129
7	0.000672868	VMware_be:8a:a7	Broadcast	ARP	42	Who has 192.168.5.7? Tell 192.168.5.129
8	0.000807430	VMware_be:8a:a7	Broadcast	ARP	42	Who has 192.168.5.8? Tell 192.168.5.129
9	0.000944564	VMware_be:8a:a7	Broadcast	ARP	42	Who has 192.168.5.9? Tell 192.168.5.129
10	0.001072704	VMware_be:8a:a7	Broadcast	ARP	42	Who has 192.168.5.10? Tell 192.168.5.129
11	0.001205426	VMware_be:8a:a7	Broadcast	ARP	42	Who has 192.168.5.11? Tell 192.168.5.129
12	0.001493198	VMware_be:8a:a7	Broadcast	ARP	42	Who has 192.168.5.14? Tell 192.168.5.129
13	0.001610320	VMware_be:8a:a7	Broadcast	ARP	42	Who has 192.168.5.15? Tell 192.168.5.129
14	0.100546747	VMware_be:8a:a7	Broadcast	ARP	42	Who has 192.168.5.18? Tell 192.168.5.129
15	0.100696845	VMware_be:8a:a7	Broadcast	ARP	42	Who has 192.168.5.19? Tell 192.168.5.129
16	0.100871235	VMware_be:8a:a7	Broadcast	ARP	42	Who has 192.168.5.20? Tell 192.168.5.129
17	0.101282137	VMware_be:8a:a7	Broadcast	ARP	42	Who has 192.168.5.23? Tell 192.168.5.129
18	0.101442897	VMware_be:8a:a7	Broadcast	ARP	42	Who has 192.168.5.24? Tell 192.168.5.129
19	0.101642631	VMware_be:8a:a7	Broadcast	ARP	42	Who has 192.168.5.25? Tell 192.168.5.129

Những host đang hoạt động sẽ gửi gói tin quay lại:



tcp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.5.129	192.168.5.2	TCP	74	49064 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
4	0.000359583	192.168.5.2	192.168.5.129	TCP	60	80 → 49064 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
164	1.312029131	192.168.5.129	192.168.5.2	TCP	74	49066 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
165	1.313098239	192.168.5.2	192.168.5.129	TCP	60	80 → 49066 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
167	1.315920410	192.168.5.129	192.168.5.254	TCP	74	59820 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
168	1.316145312	192.168.5.129	192.168.5.1	TCP	74	34156 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
169	1.316868554	192.168.5.1	192.168.5.129	TCP	66	80 → 34156 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS
170	1.316944614	192.168.5.129	192.168.5.1	TCP	54	34156 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
183	1.322944512	192.168.5.129	192.168.5.1	TCP	54	34156 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
342	1.733056582	192.168.5.129	192.168.5.133	TCP	74	43218 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
348	1.737095296	192.168.5.133	192.168.5.129	TCP	74	80 → 43218 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=
349	1.737135596	192.168.5.129	192.168.5.133	TCP	66	43218 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=12
350	1.737275054	192.168.5.129	192.168.5.133	TCP	74	43710 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
351	1.737481029	192.168.5.129	192.168.5.133	TCP	66	43218 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv
352	1.737726050	192.168.5.133	192.168.5.129	TCP	60	443 → 43710 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
463	2.416299859	192.168.5.129	192.168.5.254	TCP	74	59826 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
464	2.416489553	192.168.5.129	192.168.5.254	TCP	74	36072 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
502	2.516584470	192.168.5.129	192.168.5.254	TCP	74	36074 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK

Câu 34:

Dùng lệnh ifconfig trên máy metasploitable2 để xem ip máy:

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:18:b6:48
          inet addr:192.168.5.133  Bcast:192.168.5.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe18:b648/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2233 errors:7 dropped:43 overruns:0 frame:0
          TX packets:3545 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:136752 (133.5 KB)  TX bytes:267544 (261.2 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:198 errors:0 dropped:0 overruns:0 frame:0
          TX packets:198 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:71033 (69.3 KB)  TX bytes:71033 (69.3 KB)
```

Sau đó trên máy kali, ta dùng lệnh nmap để quét và liệt kê các dịch vụ, banner đang chạy trên máy metasploitable2.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT -sV -A 192.168.5.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-13 22:19 EDT
Nmap scan report for 192.168.5.133
Host is up (0.0027s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.5.129
|      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
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)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2022-10-14T02:20:12+00:00; +1s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
```

```
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceN
ame=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, ENHA
NCEDSTATUSCODES, 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      34568/udp   mountd
|   100005  1,2,3      53411/tcp   mountd
|   100021  1,3,4      52656/tcp   nlockmgr
|   100021  1,3,4      55036/udp   nlockmgr
|   100024  1          44485/tcp   status
|_  100024  1          51513/udp   status
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 rlogind
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
```

```
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinc
ame=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
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-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:
pe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h00m00s, deviation: 2h00m00s, median: 0s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-10-13T22:20:03-04:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.62 seconds
```

Câu 35:

Di chuyển tới /usr/share/nmap/scripts để xem các tập lệnh NSE có sẵn hoặc ta có thể tham khảo ở: **https://nmap.org/book/nse.html**

Script: default and safe

Loads those scripts that are in *both* the default and safe categories.

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap 192.168.5.133 --script "default and safe"
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-20 07:25 EDT
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.16% done; ETC: 07:26 (0:00:02 remaining)
Nmap scan report for 192.168.5.133
Host is up (0.0023s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.5.129
|      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
22/tcp   open  ssh
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet
25/tcp   open  smtp
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
NHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvi
ceName=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
| sslv2:
|   SSLv2 supported
```

```
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ssl-date: 2022-10-20T11:25:49+00:00; -3s from scanner time.
53/tcp   open  domain
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind
| 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      35863/udp   mountd
|   100005  1,2,3      51157/tcp   mountd
|   100021  1,3,4      35133/udp   nlockmgr
|   100021  1,3,4      49552/tcp   nlockmgr
|   100024  1          36069/tcp   status
|_  100024  1          47872/udp   status
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:
```

```
5432/tcp open  postgresql
|_ssl-date: 2022-10-20T11:25:35+00:00; -3s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrPro
ceName=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-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  unknown
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 00:0C:29:18:B6:48 (VMware)

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: 2022-10-20T07:25:17-04:00
|_clock-skew: mean: 59m56s, deviation: 2h00m00s, median: -3s
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unk
n)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Nmap done: 1 IP address (1 host up) scanned in 75.18 seconds
```

Script: unsual-port.nse

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sV 192.168.5.133 --script=unusual-port.nse

Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-20 07:41 EDT
Nmap scan report for 192.168.5.133
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 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
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      35863/udp   mountd
|   100005  1,2,3      51157/tcp   mountd
|   100021  1,3,4      35133/udp   nlockmgr
|   100021  1,3,4      49552/tcp   nlockmgr
|   100024  1          36069/tcp   status
|_  100024  1          47872/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
|_unusual-port: tcpwrapped unexpected on port tcp/514
1099/tcp open  java-rmi    GNU Classpath grmiregistry
```

```
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
|_unusual-port: tcpwrapped unexpected on port tcp/514
1099/tcp open  java-rmi    GNU Classpath grmiregistry
|_unusual-port: java-rmi unexpected on port tcp/1099
1524/tcp open  bindshell   Metasploitable root shell
|_unusual-port: bindshell unexpected on port tcp/1524
2049/tcp open  nfs         2-4 (RPC #100003)
|_unusual-port: rpcbind unexpected on port tcp/2049
2121/tcp open  ftp         ProFTPD 1.3.1
|_unusual-port: ftp unexpected on port tcp/2121
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
MAC Address: 00:0C:29:18:B6:48 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE
: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.87 seconds
```

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

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 .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/Tên Cá nhân đã đăng ký với GV).

  *Ví dụ: [*NT101.K11.ANTT*]-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.
- 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. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

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

HẾT