

Báo cáo LAB 2 - Thu thập thông tin (về nhà)

An toàn Mạng – NT140.P11.ANTN

Ngày báo cáo: 10/10/2024

GVHD: Nghi Hoàng Khoa

Tên nhóm: 5

STT	Họ và tên	MSSV	Nội dung công việc đã làm
1	Vũ Ngọc Quốc Khánh	22520661	19,20,21,22,23,24,26,27,28
2	Nguyễn Đức Luân	22520825	29,30,31,32,33,34,35
3	Đào Hoàng Phúc	22521110	9,10,11,12,13,14,15,16,17,18

Câu 9

Tên bài

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

Các bước thực hiện

Các từ khóa thường gặp là: intext, filetype, inurl, intitle, allintitle, site

Câu 10

Tên bài

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

Các bước thực hiện

Truy cập trang ctsv.uit.edu.vn, ta điền vào từ khóa Học bổng

Dòng tra cứu <https://ctsv.uit.edu.vn/bai-viet/danh-sach-sinh-vien-nhan-hoc-bong-hk1-2022-2023> xuất hiện trên trang web là thông tin công khai, có thể vào mà không cần đăng nhập

The screenshot shows a news article titled "Danh sách sinh viên nhận học bổng HK1 2022-2023". The article lists various scholarships, including the "Khuyễn khích học tập HK2 năm học 2021-2022" (worth 6,600,000 VND) and "Học bổng Chương trình tiên tiến - Chương trình Chất lượng cao HK2 năm học 2021-2022" (worth 6,600,000 VND). It also mentions the "Học bổng Tuyển sinh HK1 năm học 2022-2023" and "Học bổng Tài năng ngành Khoa học Máy tính HK1 năm học 2022-2023". A sidebar on the left contains a list of news items and a link to "Xem tất cả".

Bấm vào file https://ctsv.uit.edu.vn/sites/default/files/202212/1048_kkht.pdf cho ta danh sách các sinh viên nhận được học bổng KKHT

The PDF document is titled "DANH SÁCH SINH VIÊN ĐƯỢC NHẬN HỌC BỔNG KHUYẾN KHÍCH HỌC TẬP HỌC KỲ 2 NĂM HỌC 2021-2022". It includes a note: "(Ban hành kèm theo Quyết định số: 148/QĐ-DHCNTT, ngày 6 tháng 12 năm 2022)". The table lists 20 students with their MSSV, Họ tên, Lớp, Xếp loại, Số tiền, and Ghị chú.

TT	MSSV	Họ tên	Lớp	Xếp loại	Số tiền	Ghi chú
1	19520958	Phạm Ngọc Thành	ATCL2019	Giỏi	6,600,000	
2	19521184	Nguyễn Thị Trường An	ATCL2019	Giỏi	6,600,000	
3	19521190	Bùi Đức Anh	ATCL2019	Giỏi	6,600,000	
4	20521862	Trần Tân Tài	ATCL2020	Giỏi	6,600,000	
5	20522177	Hà Triệu Yến Vy	ATCL2020	Giỏi	6,600,000	
6	20521146	Nguyễn Đoàn Thiên Cung	ATCL2020	Giỏi	6,600,000	
7	20521830	Trần Hoài Rin	ATCL2020	Giỏi	6,600,000	
8	21522090	Lê Xuân Hoàng	ATCL2021	Xuất sắc	14,400,000	
9	21521987	Đoàn Thị Ánh Dương	ATCL2021	Xuất sắc	14,400,000	
10	21520353	Nguyễn Ngọc Trà My	ATCL2021	Giỏi	13,200,000	
11	21521520	Huỳnh Minh Tân Tiến	ATCL2021	Giỏi	13,200,000	
12	21522694	Lê Thị Huyền Trang	ATCL2021	Giỏi	13,200,000	
13	21520679	Đoàn Hải Đăng	ATCL2021	Xuất sắc	14,400,000	
14	19522137	Ngô Đức Hoàng Sơn	ATTN2019	Giỏi	6,600,000	
15	19521815	Trần Đức Lương	ATTN2019	Xuất sắc	7,200,000	
16	20520173	Bùi Tân Hải Đăng	ATTN2020	Giỏi	6,600,000	
17	20520377	Trần Bảo Ân	ATTN2020	Giỏi	6,600,000	
18	21520128	Phan Huy Vũ	ATTN2021	Xuất sắc	14,400,000	
19	21520377	Liêu Minh Nhật	ATTN2021	Xuất sắc	14,400,000	
20	19521439	Lê Thị Mỹ Duyên	ATTT2019	Giỏi	6,600,000	

Ở đây lộ ra MSSV, lớp và số tiền nhận của các sinh viên, vốn là thông tin nhạy cảm

Câu 11

Tên bài

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

Các bước thực hiện

Thực hiện việc tra cứu trên <https://searchdns.netcraft.com/>

The screenshot shows a web browser window with the URL <https://searchdns.netcraft.com/>. The page title is "Search Web by Domain". Below it, a sub-header says "Explore websites visited by users of the Netcraft extensions". A search bar contains the query "Site contains www.megacorpone.com". A "SEARCH" button is visible below the search bar. A "Search tips" link is located at the bottom right of the search area. The Netcraft logo is at the bottom of the page.

Ta thu được các thông tin sau:

The screenshot shows the search results for "Hostnames matching www.megacorpone.com". It displays 1 result. The table includes columns for Rank, Site, First seen, Netblock, OS, and Site Report. The single result is for rank 49693, site www.megacorpone.com, first seen in March 2013, netblock OVH Hosting, Inc., OS Linux - Debian, and a Site Report link.

Rank	Site	First seen	Netblock	OS	Site Report
49693	www.megacorpone.com	March 2013	OVH Hosting, Inc.	Linux - Debian	Site Report

Máy chủ ứng dụng chạy trên OS là Linux-Debian

Câu 12

Tên bài

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

Các bước thực hiện

Tiến hành phân giải IP của các domain yêu cầu bằng module `recon/hosts-hosts/resolve`

```
[recon-ng] [default][resolve] > options set SOURCE www.megacorpone.com
SOURCE => www.megacorpone.com
[recon-ng] [default][resolve] > run
[recon-ng] [default][resolve] > 149.56.244.87
[recon-ng] [default][resolve] > options set SOURCE support.megacorpone.com
SOURCE => support.megacorpone.com
[recon-ng] [default][resolve] >
[*] support.megacorpone.com => 167.114.21.74
[recon-ng] [default][resolve] > options set SOURCE      intranet.megacorpone.com
SOURCE > intranet.megacorpone.com
[recon-ng] [default][resolve] > run
[*] intranet.megacorpone.com => 167.114.21.67
[recon-ng] [default][resolve] > options set SOURCE admin.megacorpone.com
SOURCE => admin.megacorpone.com
[recon-ng] [default][resolve] > run
[*] admin.megacorpone.com => 167.114.21.64
[recon-ng] [default][resolve] > [REDACTED]
```

Câu 13

Tên bài

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

Các bước thực hiện

Tải và sử dụng modules discovery/info_disclosure/interesting_files để lấy các file thú vị ở những vị trí dễ đoán

```
[recon-ng] [default] > marketplace info discovery/info_disclosure/interesting_files
+-----+
| path      | discovery/info_disclosure/interesting_files
| name      | Interesting File Finder
| author    | Tim Tomes (@lammaster53), thrapt (thrapt@gmail.com), Jay Turla (@shipcod3), and Mark Jeffery
| version   | 1.2
| last updated | 2021-10-04
| description | Checks hosts for interesting files in predictable locations.
| required_keys | []
| dependencies | []
| files     | ['interesting_files_verify.csv']
| status    | not installed
+-----+
[recon-ng] [default] > marketplace install discovery/info_disclosure/interesting_files
(*) Module installed: discovery/info_disclosure/interesting_files
(*) Reloading modules...
[recon-ng] [default] > modules load discovery/info_disclosure/interesting_files
[recon-ng] [default] [interesting_files] >
[recon-ng] [default] [interesting_files] > options set SOURCE uit.edu.vn
SOURCE => uit.edu.vn
[recon-ng] [default] [interesting_files] > run
(*) http://uit.edu.vn:80/robots.txt => 200. 'robots.txt' found!
(*) http://uit.edu.vn:80/sitemap.xml => 200. 'sitemap.xml' found!
(*) http://uit.edu.vn:80/sitemap.xml.gz => 404
(*) http://uit.edu.vn:80/crossdomain.xml => 404
(*) http://uit.edu.vn:80/phpinfo.php => 404
(*) http://uit.edu.vn:80/test.php => 404
(*) http://uit.edu.vn:80/elmah.axd => 404
(*) http://uit.edu.vn:80/server-status => 404
(*) http://uit.edu.vn:80/jmx-console/ => 404
(*) http://uit.edu.vn:80/admin-console/ => 404
(*) http://uit.edu.vn:80/web-console/ => 200. 'web-console/' found but unverified.
2 interesting files found.
Files downloaded to '/home/kali/.recon-ng/workspaces/default/'
[recon-ng] [default] [interesting_files] > 
```

```
[(kali㉿kali)-~/.recon-ng/workspaces/default]
└─$ ls
config.dat  data.db  http_uit.edu.vn_robots.txt  http_uit.edu.vn_sitemap.xml
```

Content của file http_uit.edu.vn_robots.txt

```
#  
# robots.txt  
#  
# This file is to prevent the crawling and indexing of certain parts  
# of your site by web crawlers and spiders run by sites like Yahoo!  
# and Google. By telling these "robots" where not to go on your site,  
# you save bandwidth and server resources.  
#  
# This file will be ignored unless it is at the root of your host:  
# Used:    http://example.com/robots.txt  
# Ignored: http://example.com/site/robots.txt  
#  
# For more information about the robots.txt standard, see:  
# http://www.robotstxt.org/robotstxt.html
```

```
User-agent: *
Crawl-delay: 10
# CSS, JS, Images
Allow: /misc/*.css$
Allow: /misc/*.css?
Allow: /misc/*.js$
Allow: /misc/*.js?
```

```
Allow: /misc/*.gif
Allow: /misc/*.jpg
Allow: /misc/*.jpeg
Allow: /misc/*.png
Allow: /modules/*.css$
Allow: /modules/*.css?
Allow: /modules/*.js$
Allow: /modules/*.js?
Allow: /modules/*.gif
Allow: /modules/*.jpg
Allow: /modules/*.jpeg
Allow: /modules/*.png
Allow: /profiles/*.css$
Allow: /profiles/*.css?
Allow: /profiles/*.js$
Allow: /profiles/*.js?
Allow: /profiles/*.gif
Allow: /profiles/*.jpg
Allow: /profiles/*.jpeg
Allow: /profiles/*.png
Allow: /themes/*.css$
Allow: /themes/*.css?
Allow: /themes/*.js$
Allow: /themes/*.js?
Allow: /themes/*.gif
Allow: /themes/*.jpg
Allow: /themes/*.jpeg
Allow: /themes/*.png
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
```

```

Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=filter/tips/
Disallow: /?q=node/add/
Disallow: /?q=search/
Disallow: /?q=user/password/
Disallow: /?q=user/register/
Disallow: /?q=user/login/
Disallow: /?q=user/logout/

```

Câu 14

Tên bài

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

Các bước thực hiện

Truy cập vào github thầy Vũ Tuấn Hải và tìm được repository của trang web liên quan đến Ban học tập Công nghệ phần mềm

The screenshot shows a GitHub repository page for 'FrontendStudyingBoard' (Public). The repository has 20 branches and 228 commits. The commits include various refactoring and dependency updates. The repository description is 'Website for Studying board' and it links to 'bht-cnpm-uit-edu-vn.now.sh'. The repository has 1 star, 1 watching, and 0 forks.

Thực hiện git clone repository, cd vào trong đó và sử dụng công cụ Gitleaks với lệnh `gitleaks detect -v` thì ta thấy rằng có 1 leak được tìm thấy trong code, cụ thể là lỗ API

Key

```
(kali㉿kali)-[~]
└─$ 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% (44/44), done.
remote: Total 5085 (delta 51), reused 8 (delta 8), pack-reused 5012 (from 1)
Receiving objects: 100% (5085/5085), 6.68 MiB | 1.44 MiB/s, done.
Resolving deltas: 100% (3340/3340), done.

(kali㉿kali)-[~]
└─$ cd FrontendStudyingBoard
(kali㉿kali)-[~/FrontendStudyingBoard]
└─$ gitleaks detect -v

Sorry, We're having trouble getting your pages back.

Finding: arikey -ngs fnd17zvx70gflf0dsauilk0bg1crokafq4filexers We are having trouble restoring your last browsing session. Select Restore Session to try again.
Secret: gitleaks17zvx70gflf0dsauilk0bg1crokafq4filexers
RuleID: generic-api-key
Entropy: 4.490602
File: src/component/layout/create_post.js
Line: 29
Commit: 1a3aee322de8c07ce0569d661464d17690b14f3a
Author: vutuanhai237
Email: 43282025+vutuanhai237@users.noreply.github.com
Date: 2028-04-28T15:30:13Z
Fingerprint: 1a3aee322de8c07ce0569d661464d17690b14f3a:src/component/layout/create_post.js:generic-api-key:0

12:01PM INF 17/22 commits scanned.
12:01PM INF scan completed in 15.7s
12:01PM WRN leaks found: 1

(kali㉿kali)-[~/FrontendStudyingBoard]
└─$
```

Câu 15

Tên bài

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

Các bước thực hiện

Thực hiện search trên Shodan với từ khóa Router

The screenshot shows the Shodan search interface with the query 'Router' entered. The results page displays 1,391,257 total results. A world map shows the top countries where routers were found, with China being the most prominent at 320,954. Below the map, a table lists the top ports: 80, 23, 443, and 161. On the right side, there are two detailed SSL certificate sections for 'Heroku | Application Error' and 'Home'. The 'Heroku' section shows an SSL certificate issued by Amazon RSA 2048 M02 to 'herokuapp.com'. The 'Home' section shows an SSL certificate issued by Let's Encrypt to 'deklarinet.cms.socialschools.nl'.

Theo như kết quả tìm kiếm trong hình có vẻ như có ứng dụng trên nền tảng Heroku gặp lỗi

Câu 16

Tên bài

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

Các bước thực hiện

- Shodan: Tập trung vào các thiết bị kết nối Internet, bao gồm máy chủ, camera, router, và các thiết bị IoT. Shodan cho phép người dùng tìm kiếm thông tin về cấu hình và lỗ hổng bảo mật của các thiết bị này.
- Google/Bing: Tìm kiếm các trang web, bài viết, hình ảnh, video và thông tin trên Internet nói chung. Nội dung tìm kiếm thường liên quan đến thông tin văn bản và hình ảnh hơn là các thiết bị.

Câu 17

Tên bài

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

Các bước thực hiện

Ta tìm được 27 email của UIT với lệnh theHarvester -d uit.edu.vn -b yahoo

```
(kali㉿kali)-[~/Desktop/gitleaks]
$ theHarvester -d uit.edu.vn -b yahoo
[*] No IPs found.
[*] No emails found.
[*] No hosts found.

=====
[*] Target: uit.edu.vn
[*] Searching Yahoo, Google, Bing, Baidu...
[*] No IPs found.
[*] Emails found: 27
01234567@gm.uit.edu.vn
cttd@uit.edu.vn
cttd@uit.edu.vn
cttd@uit.edu.vn
emailinfo@uit.edu.vn
hung1@uit.edu.vn
huynh@uit.edu.vn
infotech@uit.edu.vn
info@uit.edu.vn
khangntm@uit.edu.vn
minhdt@uit.edu.vn
phongdat@uit.edu.vn
phongdat@uit.edu.vn
phon1@uit.edu.vn
phuong1tm@uit.edu.vn
ptn.htt@uit.edu.vn
quangviet@uit.edu.vn
qladm@uit.edu.vn
quantu@uit.edu.vn
sangv@uit.edu.vn
thuanh@uit.edu.vn
thuyenv@uit.edu.vn
thuyentd@uit.edu.vn
tinhv@uit.edu.vn
tuyensinh@uit.edu.vn
vpdb@uit.edu.vn
vand@uit.edu.vn
```

Câu 18

Tên bài

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

Các bước thực hiện

Thực hiện câu lệnh `theHarvester -d uit.edu.vn -b duckduckgo` cho ra kết quả chỉ có 1 email

```
(kali㉿kali)-[~/Desktop/gitleaks]
└─$ theHarvester -d uit.edu.vn -b duckduckgo
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
*****
* [!] TheHarvester 4.6.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****
[*] Target: uit.edu.vn
[*] Searching Duckduckgo.
[*] No IPs Found.
[*] No Domains Found.
[*] Emails Found: 1
info@uit.edu.vn
```

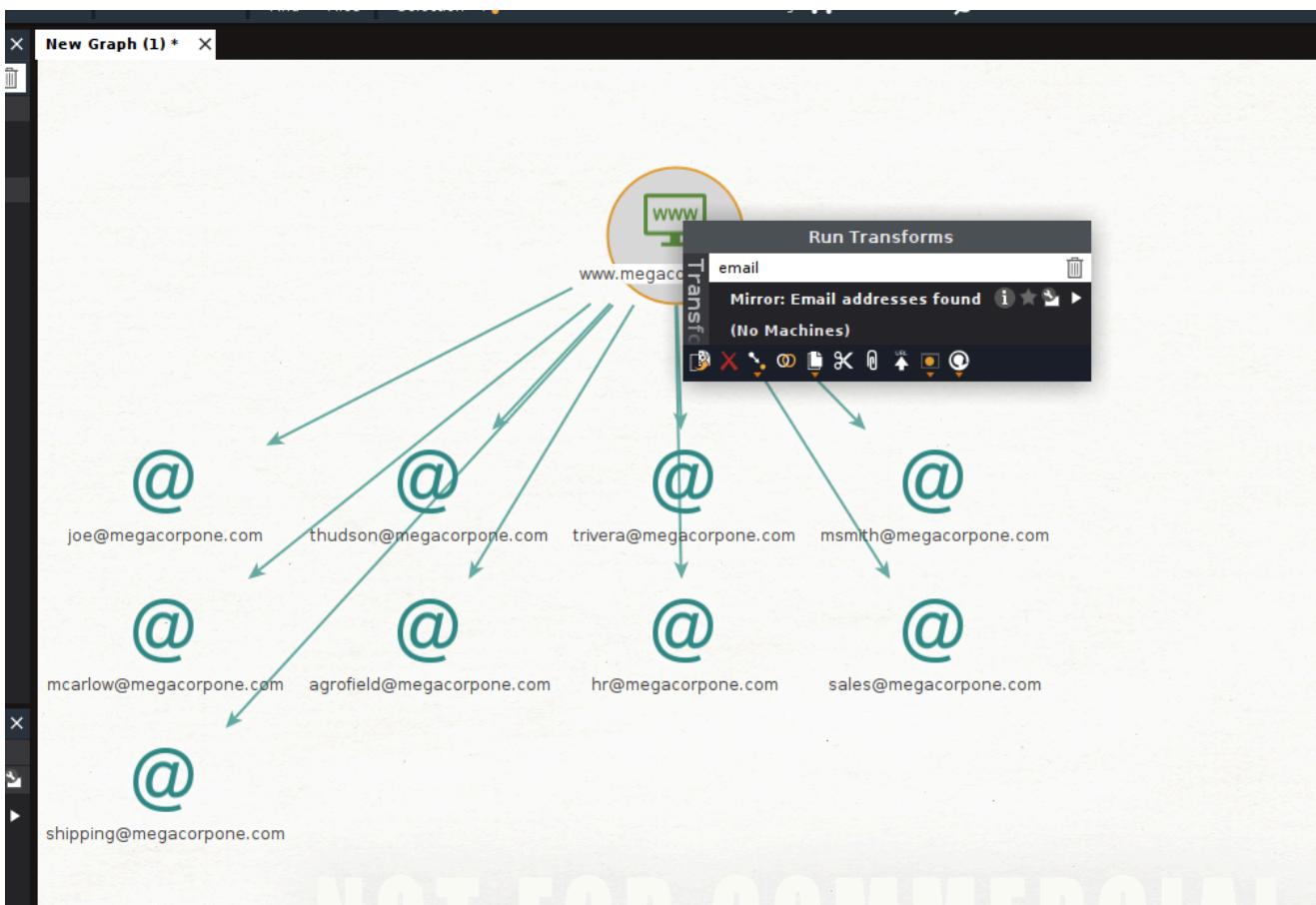
Nên kết quả với nguồn của Yahoo là tốt hơn Duckduckgo trong trường hợp này

Câu 19

Tên bài

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

Các bước thực hiện



- Trong các transform của Maltego, có một transform để tìm Email.

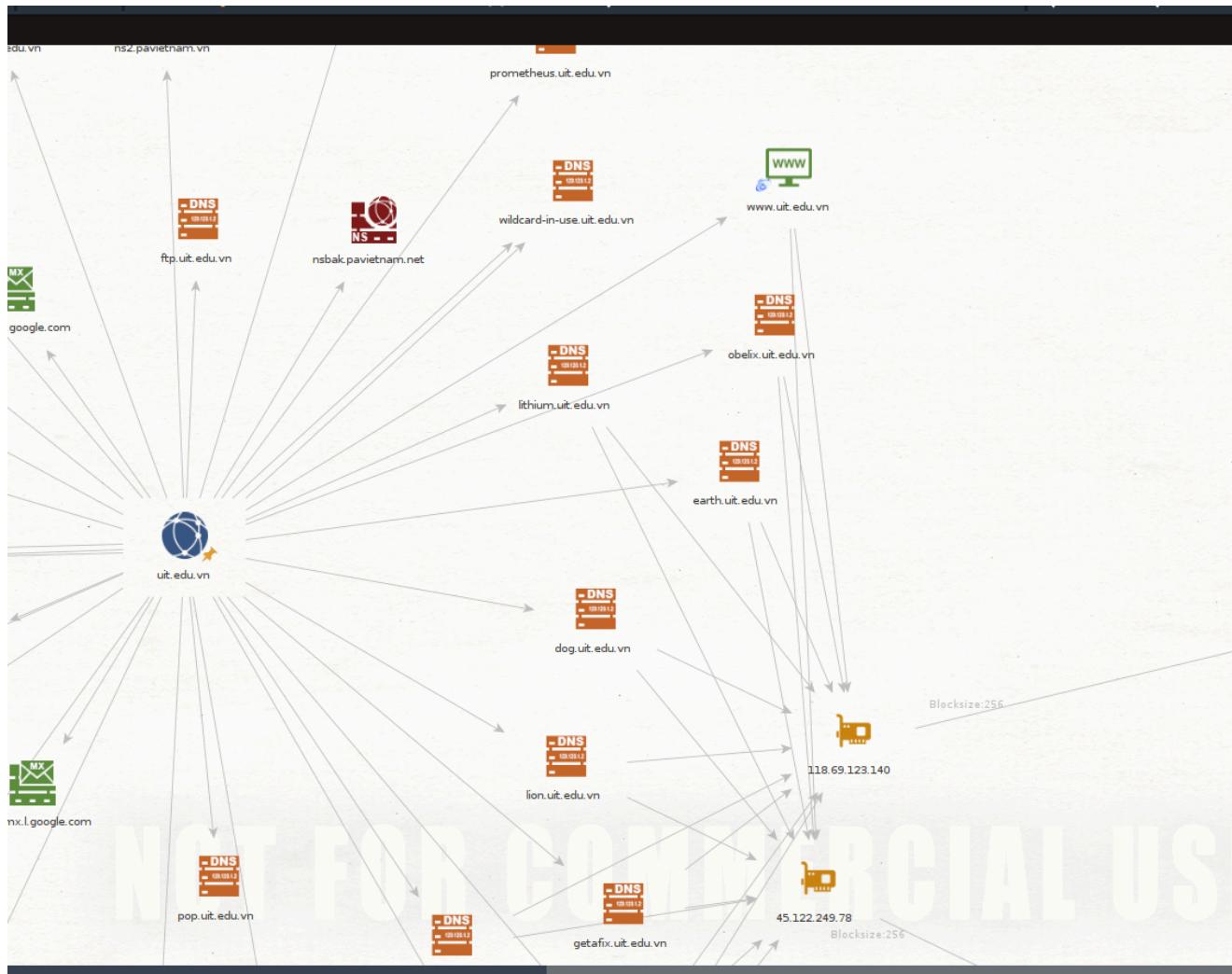
Câu 20

Tên bài

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

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

b. Các website và địa chỉ IP tương ứng



Câu 21

Tên bài

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

Các bước thực hiện

Trên trang web của [Cloudflare](#) có liệt kê các bản ghi của DNS

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.](#)

- **AFSDB record** - This record is used for clients of the Andrew File System (AFS) developed by Carnegie Mellon. The AFSDB record functions to find other AFS cells.
- **APL record** - The ‘address prefix list’ is an experimental record that specifies lists of address ranges.
- **CAA record** - This is the ‘certification authority authorization’ record, it allows domain owners state which certificate authorities can issue certificates for that domain. If no CAA record exists, then anyone can issue a certificate for the domain. These records are also inherited by subdomains.
- **DNSKEY record** - The ‘[DNS Key Record](#)’ contains a [public key](#) used to verify [Domain Name System Security Extension \(DNSSEC\)](#) signatures.
- **CDNSKEY record** - This is a child copy of the DNSKEY record, meant to be transferred to a parent.
- **CERT record** - The ‘certificate record’ stores public key certificates.
- **DCHID record** - The ‘DHCP Identifier’ stores info for the Dynamic Host Configuration Protocol (DHCP), a standardized network protocol used on IP networks.
- **DNAME record** - The ‘delegation name’ record creates a domain alias, just like CNAME, but this alias will redirect all subdomains as well. For instance if the owner of ‘example.com’ bought the domain ‘website.net’ and gave it a DNAME record that points to ‘example.com’, then that pointer would also extend to ‘blog.website.net’ and any other subdomains.

- **HIP record** - This record uses 'Host identity protocol', a way to separate the roles of an IP address; this record is used most often in mobile computing.
- **IPSECKEY record** - The 'IPSEC key' record works with the [Internet Protocol Security \(IPSEC\)](#), an end-to-end security protocol framework and part of the Internet Protocol Suite [\(TCP/IP\)](#).
- **LOC record** - The 'location' record contains geographical information for a domain in the form of longitude and latitude coordinates.
- **NAPTR record** - The 'name authority pointer' record can be combined with an [SRV record](#) to dynamically create URI's to point to based on a regular expression.
- **NSEC record** - The 'next secure record' is part of DNSSEC, and it's used to prove that a requested DNS resource record does not exist.
- **RRSIG record** - The 'resource record signature' is a record to store digital signatures used to authenticate records in accordance with DNSSEC.
- **RP record** - This is the 'responsible person' record and it stores the email address of the person responsible for the domain.
- **SSHFP record** - This record stores the 'SSH public key fingerprints'; SSH stands for Secure Shell and it's a cryptographic networking protocol for secure communication over an unsecure network.

Câu 22

Tên bài

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

Các bước thực hiện

Sử dụng lệnh:

```
host -t txt uit.edu.vn
host -t mx uit.edu.vn
```

```
> cd ~  
> host -t txt uit.edu.vn  
uit.edu.vn descriptive text "svp60rjlwr6s19rn9t013cfwm3xmqx7h"  
uit.edu.vn descriptive text "MS=E431E3CA3EFF5A6431E2378C924984A8A0334ABC"  
uit.edu.vn descriptive text "_ukan9w1l3iica61scp6fwumq5v6dopw"  
uit.edu.vn descriptive text "k6t321pqvf9jryb0z4n5scftph6t781"  
uit.edu.vn descriptive text "v=spf1 include:_spf.google.com ~all"  
uit.edu.vn descriptive text "sqm6y27vn74pm290pl0fq4hcr08gst5r"  
uit.edu.vn descriptive text "google-site-verification=wjArKGa37oHK083XqT2C91tPny8NLttGS0aU5pJjkIY"  
uit.edu.vn descriptive text "google-site-verification=z9wIF5gp5-YbdAQsttR2KmyHCPy3FN6Qk0G0BUWIrwc"  
> host -t mx uit.edu.vn  
uit.edu.vn mail is handled by 20 alt2.aspmx.l.google.com.  
uit.edu.vn mail is handled by 40 aspmx3.googlemail.com.  
uit.edu.vn mail is handled by 20 alt1.aspmx.l.google.com.  
uit.edu.vn mail is handled by 10 aspmx.l.google.com.  
uit.edu.vn mail is handled by 40 aspmx2.googlemail.com.  
WSL at 150ms zsh 7.7
```

Câu 23

Tên bài

Sử dụng lệnh host cho các hostname không tồn tại trong tên miền uit.edu.vn (idontexist, noexist, baithuchanhso2). Có nhận xét gì về kết quả trả về hay không? Giải thích

Các bước thực hiện

```
(anotherk@kda)-[~]$ host idontexist.uit.edu.vn  
idontexist.uit.edu.vn has address 118.69.123.140  
idontexist.uit.edu.vn has address 45.122.249.78  
  
(anotherk@kda)-[~]$ host noexist.uit.edu.vn  
noexist.uit.edu.vn has address 45.122.249.78  
noexist.uit.edu.vn has address 118.69.123.140  
  
(anotherk@kda)-[~]$ host baithuchanhso2.uit.edu.vn  
baithuchanhso2.uit.edu.vn has address 45.122.249.78  
baithuchanhso2.uit.edu.vn has address 118.69.123.140  
  
(anotherk@kda)-[~]$
```

Giải thích: Vì tên miền uit.edu.vn sử dụng bản ghi DNS wildcard, nó có thể nhận tất cả các subdomain không tồn tại và trả về địa chỉ IP mong muốn

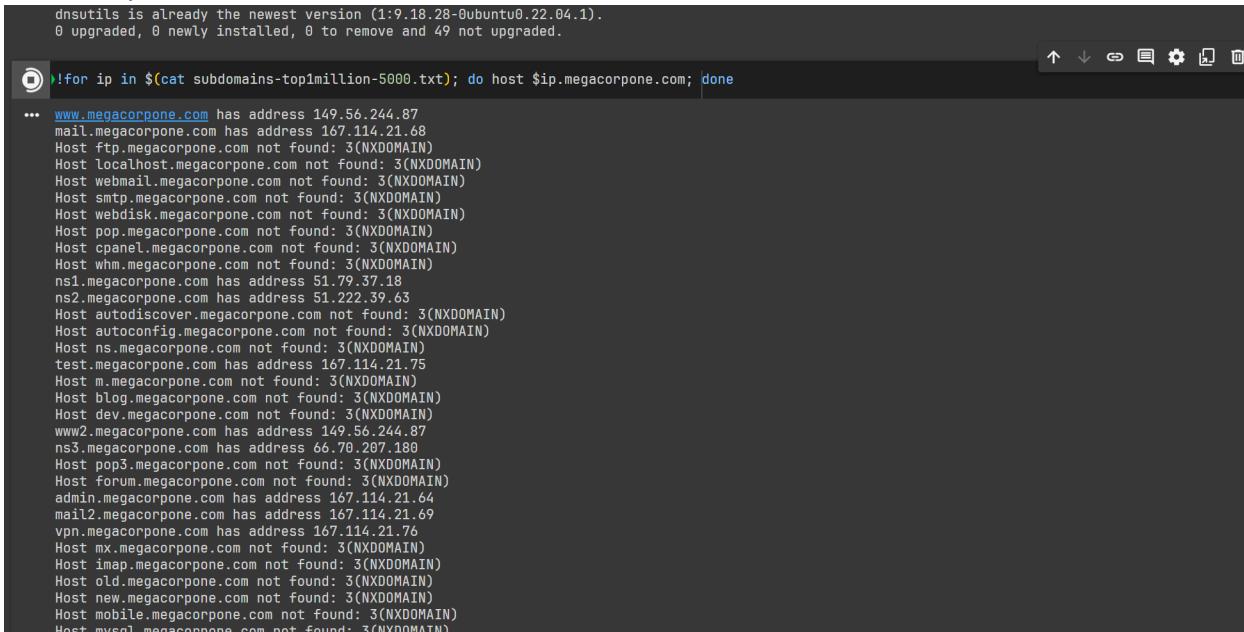
Câu 24

Tên bài

Sử dụng wordlist thông dụng khác (rockyou, seclists) để tìm kiếm các hostname hợp lệ khác của megacorpone.com

Các bước thực hiện

- Sử dụng wordlist của [seclists](#) để tìm
- Các kết quả ban đầu



```
dnsutils is already the newest version (1:9.18.28-0ubuntu0.22.04.1).
0 upgraded, 0 newly installed, 0 to remove and 49 not upgraded.

!for ip in $(cat subdomains-top1million-5000.txt); do host $ip.megacorpone.com; done

... www.megacorpone.com has address 149.56.244.87
mail.megacorpone.com has address 167.114.21.68
Host ftp.megacorpone.com not found: 3(NXDOMAIN)
Host localhost.megacorpone.com not found: 3(NXDOMAIN)
Host webmail.megacorpone.com not found: 3(NXDOMAIN)
Host smtp.megacorpone.com not found: 3(NXDOMAIN)
Host webdisk.megacorpone.com not found: 3(NXDOMAIN)
Host pop.megacorpone.com not found: 3(NXDOMAIN)
Host cpanel.megacorpone.com not found: 3(NXDOMAIN)
Host whm.megacorpone.com not found: 3(NXDOMAIN)
ns1.megacorpone.com has address 51.79.37.18
ns2.meqacorpone.com has address 51.222.39.63
Host autodiscover.megacorpone.com not found: 3(NXDOMAIN)
Host autoconfig.megacorpone.com not found: 3(NXDOMAIN)
Host ns.megacorpone.com not found: 3(NXDOMAIN)
test.megacorpone.com has address 167.114.21.75
Host m.megacorpone.com not found: 3(NXDOMAIN)
Host blog.megacorpone.com not found: 3(NXDOMAIN)
Host dev.megacorpone.com not found: 3(NXDOMAIN)
www2.megacorpone.com has address 149.56.244.87
ns3.megacorpone.com has address 66.70.207.180
Host pop3.megacorpone.com not found: 3(NXDOMAIN)
Host forum.megacorpone.com not found: 3(NXDOMAIN)
admin.megacorpone.com has address 167.114.21.64
mail2.megacorpone.com has address 167.114.21.69
vpn.megacorpone.com has address 167.114.21.76
Host mx.megacorpone.com not found: 3(NXDOMAIN)
Host imap.megacorpone.com not found: 3(NXDOMAIN)
Host old.megacorpone.com not found: 3(NXDOMAIN)
Host new.megacorpone.com not found: 3(NXDOMAIN)
Host mobile.megacorpone.com not found: 3(NXDOMAIN)
Host mysql.megacorpone.com not found: 3(NXDOMAIN)
```

- Toàn bộ kết quả có thể xem tại [đây](#)

Câu 26

Tên bài

Liệt kê danh sách các loại enumeration có thể được sử dụng cùng với tùy chọn `-t`

Các bước thực hiện

Trên trang [Github của dnsrecon](#) có ghi

- Enumerate General DNS Records for a given Domain (MX, SOA, NS, A, AAAA, SPF and TXT).

Câu 27

Tên bài

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

Các bước thực hiện

- Có thể thêm `--threads` để sử dụng đa luồng

```
dnsrecon -d megacorpone.com -D wordlist.txt -t brt --threads 4
```

```
(anotherk㉿kda)~[~/nah]
$ dnsrecon -d megacorpone.com -D subdomains-top1million-5000.txt -t brt --threads 4
[*] Using the dictionary file: subdomains-top1million-5000.txt (provided by user)
[*] brt: Performing host and subdomain brute force against megacorpone.com ...
[+] A www.megacorpone.com 149.56.244.87
[+] A mail.megacorpone.com 167.114.21.68
[+] A ns1.megacorpone.com 51.79.37.18
[+] A ns2.megacorpone.com 51.222.39.63
[+] A test.megacorpone.com 167.114.21.75
[+] A www2.megacorpone.com 149.56.244.87
[+] A ns3.megacorpone.com 66.70.207.180
[+] A admin.megacorpone.com 167.114.21.64
[+] A mail2.megacorpone.com 167.114.21.69
[+] A vpn.megacorpone.com 167.114.21.76
[+] A beta.megacorpone.com 167.114.21.65
[+] A support.megacorpone.com 167.114.21.74
[+] A intranet.megacorpone.com 167.114.21.67
[+] A router.megacorpone.com 167.114.21.70
[+] A vpn2.megacorpone.com 167.114.21.77
[+] A syslog.megacorpone.com 167.114.21.73
[+] A fs1.megacorpone.com 167.114.21.66
[+] 17 Records Found

(anotherk㉿kda)~[~/nah]
```

- Thêm option `-j` để lưu kết quả vào file json

```
dnsrecon -d megacorpone.com -D wordlist.txt -t brt --threads 4 -j
```

```
[+] 17 Records Found
(anotherk㉿kda)~[~/nah]
$ dnsrecon -d megacorpone.com -D subdomains-top1million-5000.txt -t brt --threads 4 -j
[*] Using the dictionary file: subdomains-top1million-5000.txt (provided by user)
[*] brt: Performing host and subdomain brute force against megacorpone.com ...
[+] A www.megacorpone.com 149.56.244.87
[+] A mail.megacorpone.com 167.114.21.68
[+] A ns1.megacorpone.com 51.79.37.18
[+] A ns2.megacorpone.com 51.222.39.63
[+] A test.megacorpone.com 167.114.21.75
[+] A www2.megacorpone.com 149.56.244.87
[+] A ns3.megacorpone.com 66.70.207.180
[+] A mail2.megacorpone.com 167.114.21.69
[+] A admin.megacorpone.com 167.114.21.64
[+] A vpn.megacorpone.com 167.114.21.76
[+] A beta.megacorpone.com 167.114.21.65
[+] A support.megacorpone.com 167.114.21.74
[+] A intranet.megacorpone.com 167.114.21.67
[+] 13 Records Found
[*] Saving records to JSON file: son

(anotherk㉿kda)~[~/nah]
```

Câu 28

Tên bài

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?

Các bước thực hiện

- Cú pháp của DNSEnum ngắn hơn nên phần nào đó dễ hơn
- 2 công cụ đều có kết quả chính xác như nhau
- Với cú pháp của DNSEnum sẽ cho ra kết quả nhiều hơn DNSRecon, nhưng khi ghi các option khác của DNSRecon sẽ cho ra kết quả tương tự

Câu 29

Tên bài:

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

Dùng nmap -sS để thực hiện TCP SYN scan.

Ta quét máy Metasploitable 2 có địa chỉ 192.168.110.131:

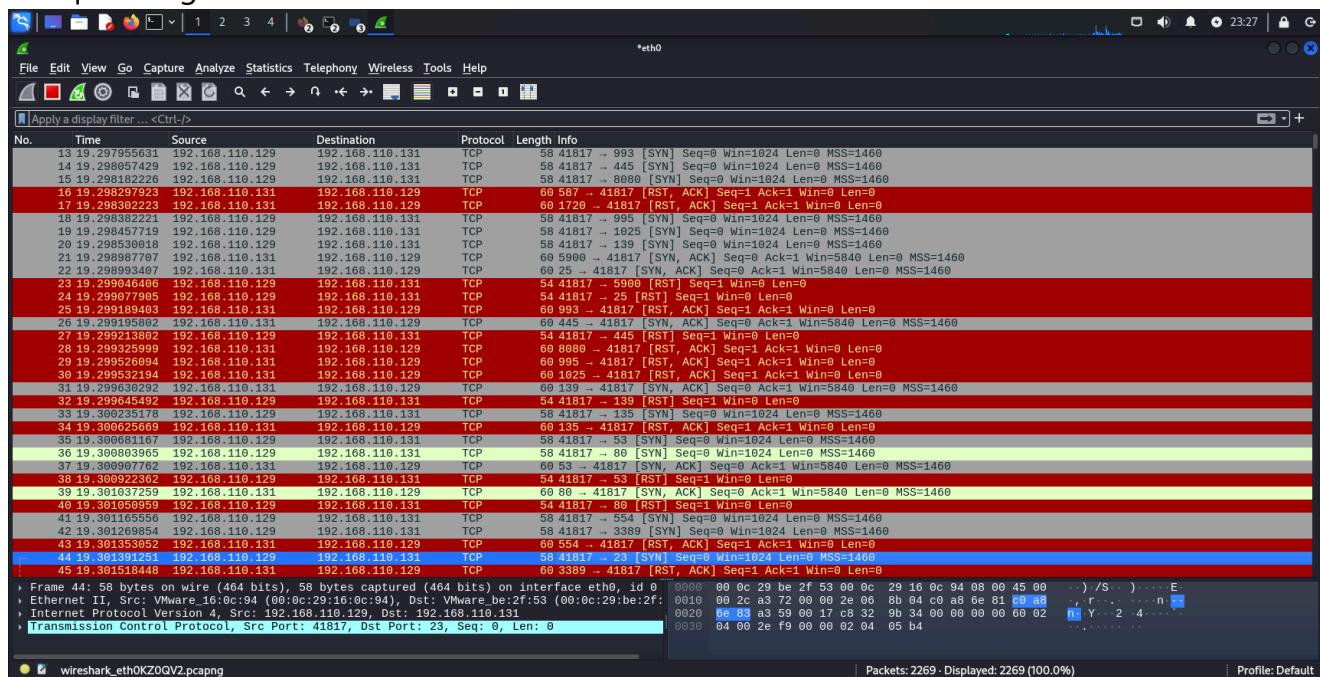
```

semloh4869@kali: ~
└$ sudo nmap -sS 192.168.110.131
[sudo] password for semloh4869:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-10-20 23:21 PDT
Nmap scan report for 192.168.110.131
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
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
513/tcp   open  rpcbind
513/tcp   open  login
514/tcp   open  shell
1699/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp open  cccproxy-ftp
3389/tcp  open  rdp
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:BE:2F:53 (VMware)

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

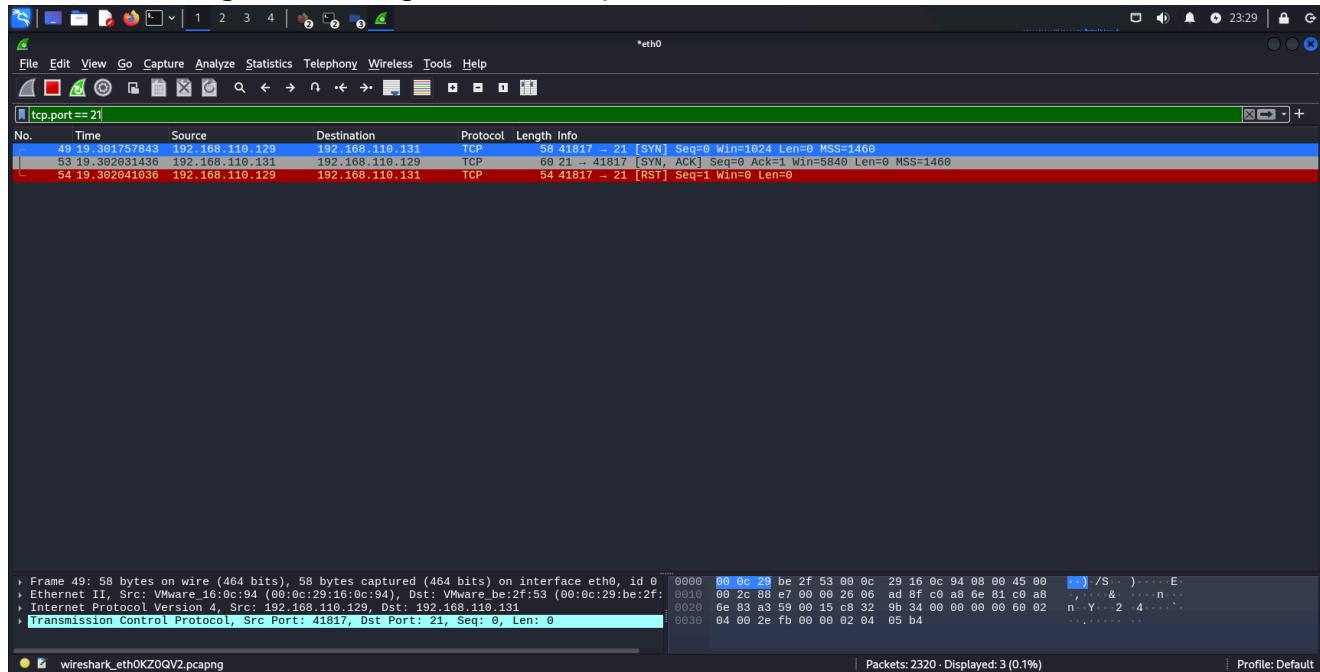
```

Kết quả bắt gói tin trên Wireshark:



Các bước thực hiện:

Phân tích cách gói tin được gửi và nhận ở port 21:

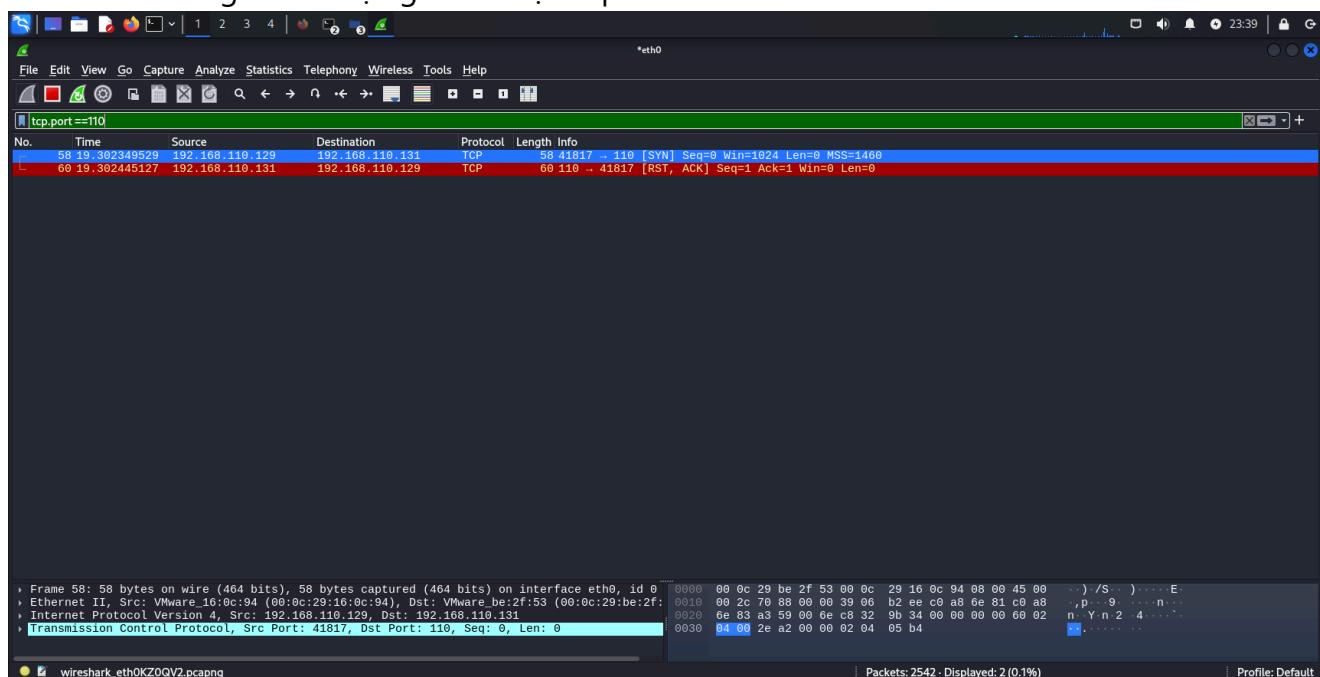


Tại gói tin thứ 49, ta có thể thấy máy của ta (192.168.110.129) thực hiện gửi gói SYN tới máy Metasploitable 2 (192.168.110.131)

Tại gói tin thứ 53, ta thấy máy Metasploitable 2 (192.168.110.131) gửi lại gói tin [SYN, ACK] tới máy của ta (192.168.110.129) nhằm thực hiện kết nối bắt tay 3 bước. Lúc này ta có thể biết được port 21 đang mở.

Tại gói tin thứ 54, máy ta (192.168.110.129) gửi gói tin RST đến máy Metasploitable 2 (192.168.110.131) nhằm kết thúc kết nối.

Phân tích cách gói tin được gửi và nhận ở port 110:



Tại gói tin thứ 58, máy ta (192.168.110.129) gửi gói tin SYN đến máy Metasploitable 2 (192.168.110.131).

Tại gói tin thứ 60, ta thấy máy Metasploitable 2 (192.168.110.131) gửi gói tin [RST, ACK] tới máy ta (192.168.110.129) và kết thúc kết nối, cho thấy rằng port 110 đang đóng.

Câu 30

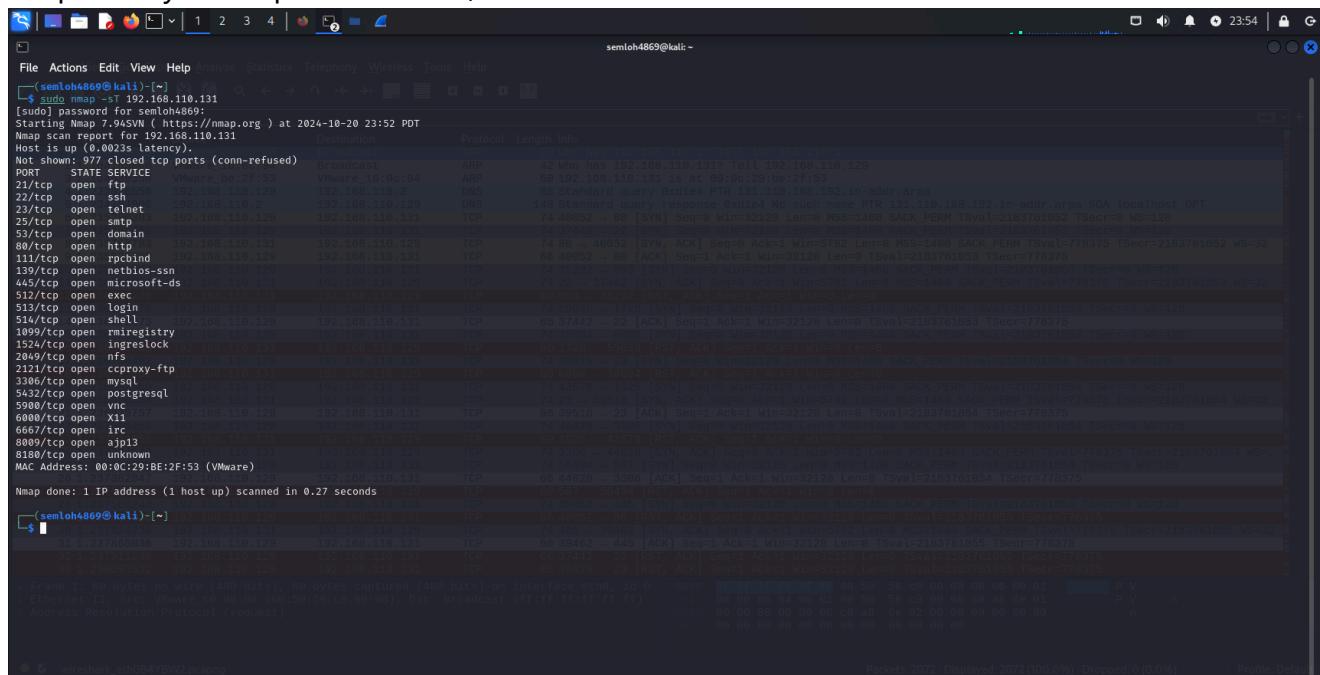
Tên bài:

Thực hiện bắt Wireshark để mô tả cách gói tin được gửi và nhận khi thực hiện TCP Connect Scan khi sử dụng Nmap.

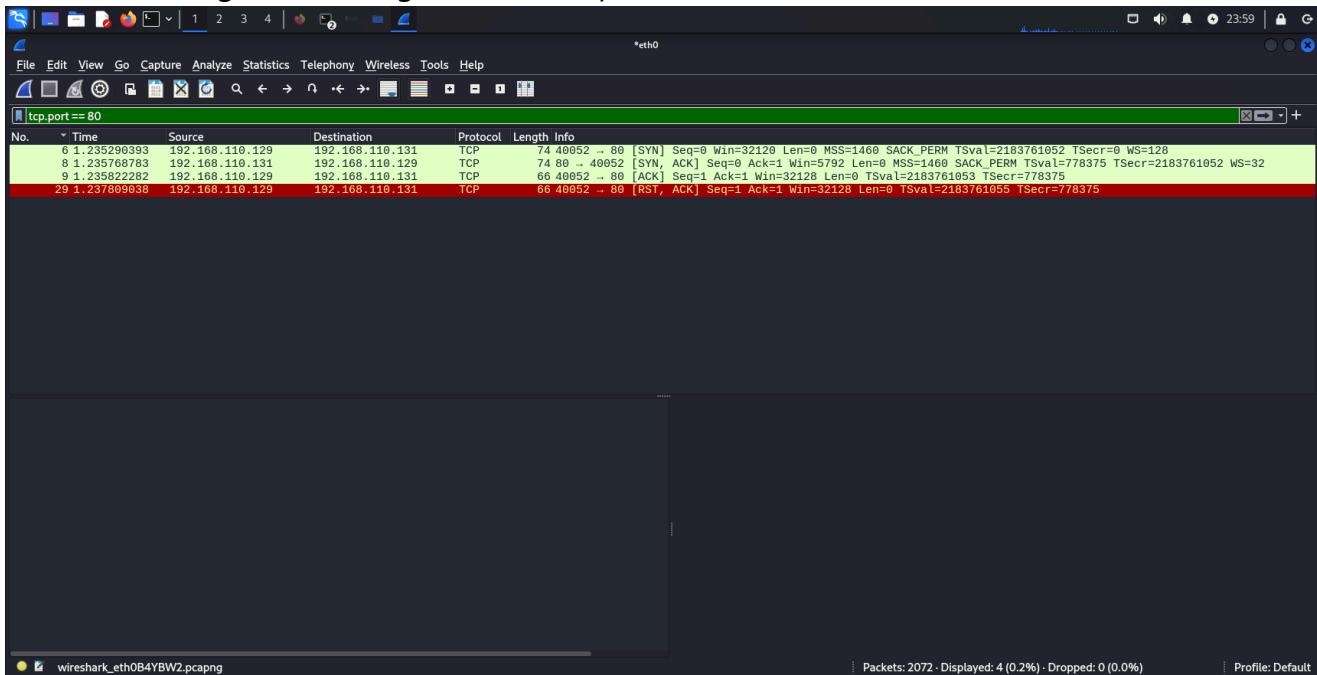
Các bước thực hiện:

Dùng nmap -sT để thực hiện TCP Connect Scan.

Ta quét máy Metasploitable có địa chỉ 192.168.110.131



Phân tích cách gói tin được gửi và nhận ở port 80:

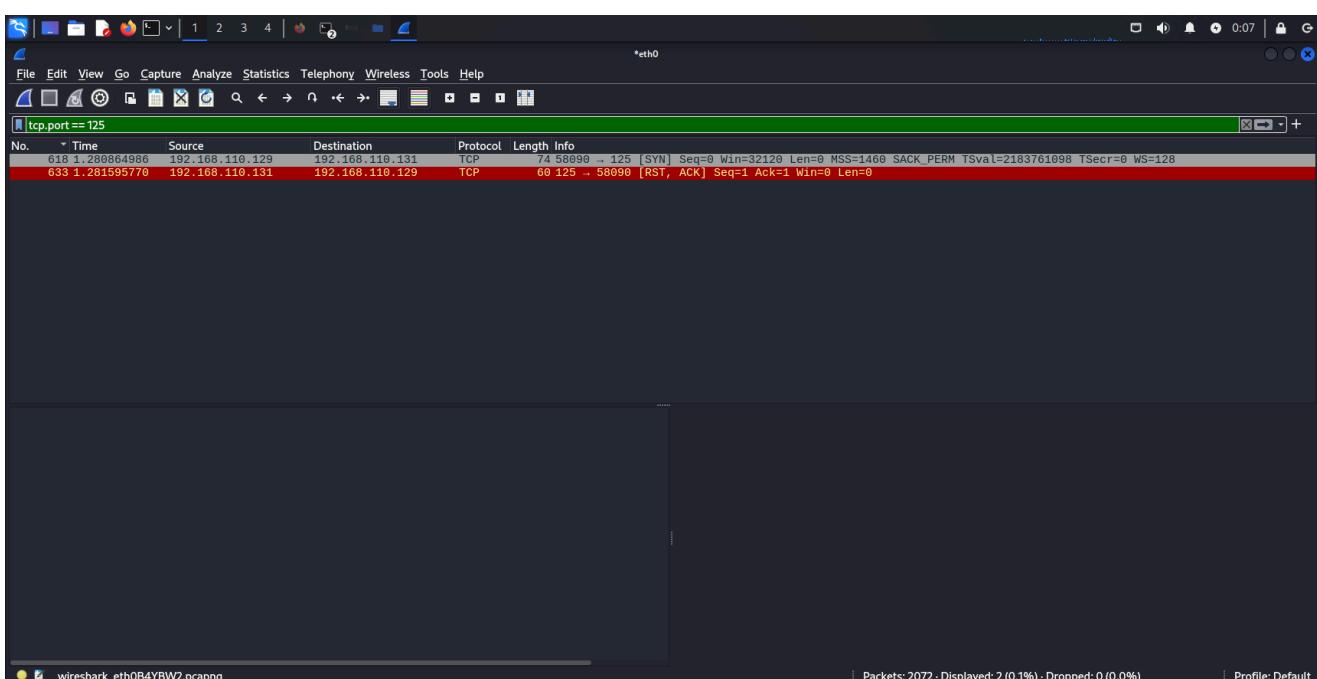


Ở gói tin thứ 6, thấy máy ta (192.168.110.131) gửi gói tin SYN đến máy Metasploitable 2 (192.168.110.131) nhằm bắt đầu kết nối bắt tay 3 bước.

Ở gói tin thứ 8, máy Metasploitable 2 (192.168.110.131) gửi gói tin [SYN, ACK] đến máy ta (192.168.110.129).

Ở gói tin thứ 9 và 21, máy ta (192.168.110.129) gửi gói ACK đến máy Metasploitable 2 (192.168.110.131) để hoàn thành việc kết nối bắt tay ba bước. Sau máy ta (192.168.110.129) gửi gói tin [RST, ACK] đến máy Metasploitable 2 (192.168.110.131) để kết thúc kết nối. Từ quá trình trên cho thấy port 80 đang mở.

Phân tích cách gói tin được gửi và nhận ở port 125:



Ở gói tin thứ 618, máy ta(192.168.110.129) gửi gói tin SYN đến máy Metasploitable 2 (192.168.110.131) nhằm bắt đầu kết nối bắt tay 3 bước.

Ở gói tin thứ 633, Metasploitable 2 (192.168.110.131) gửi gói tin [RST, ACK] đến máy ta (192.168.110.129) nhằm kết thúc kết nối. Từ đó cho thấy port 125 đang đóng.

Câu 31

Tên bài:

So sánh với phương thức SYN Scan (số lượng gói tin gửi, số lượng gói tin nhận, thời gian quét, kết quả hiển thị)

Các bước thực hiện:

Dùng công cụ Wireshark vào mục Statistics/Conversations xem ở phần IPv4 để kiểm tra số lượng gói tin gửi và nhận:

Phương thức quét	TCP Connect Scan	SYN Scan
Số lượng gói tin gửi (gói)	1048	1023
Số lượng gói tin nhận (gói)	1002	1000
Thời gian quét (giây)	0.26	0.37

Kết quả hiển thị SYN Scan:

The terminal window shows the command `sudo nmap -sS 192.168.110.131` running, followed by the Nmap scan report for the target host. The report lists various open ports and their services. The Wireshark capture window shows a single packet (the RST/ACK response) in the Conversations tab.

```
semioh4869@kali:~]$ sudo nmap -sS 192.168.110.131
Starting Nmap 7.94SYN ( https://nmap.org ) at 2024-10-21 00:21 PDT
Nmap scan report for 192.168.110.131
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftplib
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  acpica
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cccproxy-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:BE:2F:53 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

Wireshark capture details:
File: eth0TC2RV2.pcapng
Packets: 2031 - Displayed: 2031 (100.0%) - Dropped: 0 (0.0%)
Profile: Default

Kết quả hiển thị TCP Connect Scan:

The terminal window shows the output of an Nmap scan on host 192.168.110.131. The scan report includes details about open ports (e.g., 21/tcp, 22/tcp, 23/tcp, 25/tcp, 53/tcp, 80/tcp, 111/tcp, 139/tcp, 445/tcp, 512/tcp, 513/tcp, 514/tcp, 1099/tcp, 1524/tcp, 2049/tcp, 2121/tcp, 3306/tcp, 5432/tcp, 5900/tcp, 6000/tcp, 6667/tcp, 8009/tcp, 8180/tcp) and their respective states (open). The MAC address of the host is 00:0C:29:BE:2F:53 (VMware). Below the terminal is a Wireshark capture window showing network traffic on interface eth0: C:\Z7\QV2\ncand.

```
semlohb4869@kali:~$ sudo nmap -sT 192.168.110.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 00:27 PDT  [UDP:6]
Nmap scan report for 192.168.110.131
Host is up (0.002s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE          PORTS
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  cccproxy-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:BE:2F:53 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

Câu 32

Tên bài:

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

Các bước thực hiện:

Source code Python:

```
import nmap
import ipaddress

# Hàm kiểm tra tính hợp lệ của địa chỉ IP
def is_valid_ip(ip):
    try:
        ip_obj = ipaddress.ip_address(ip)
        return True
    except ValueError:
        return False

# Nhập địa chỉ IP từ người dùng
while True:
    ip_input = input("Nhập địa chỉ IP hoặc dải mạng (vd: 192.168.110.0/24): ")

    # Kiểm tra xem người dùng nhập dải mạng hay địa chỉ IP
    try:
        ip_network = ipaddress.ip_network(ip_input, strict=False)
```

```

        print(f"Dải mạng hợp lệ: {ip_network}")
        break
    except ValueError:
        print("Địa chỉ IP hoặc dải mạng không hợp lệ. Vui lòng nhập lại.")

# Khởi tạo đối tượng nmap
nm = nmap.PortScanner()

# Thực hiện quét ping với nmap
nm.scan(hosts=str(ip_network), arguments='-sn') # -sn: Quét mà không cần
quét cổng, chỉ kiểm tra host

# In ra danh sách các host hoạt động
print("\nCác host hoạt động:")
for host in nm.all_hosts():
    if nm[host].state() == 'up':
        print(f"Host {host} is up")

```

Kết quả khi chạy chương trình:

```

semloh4869@kali:~/atm
$ python3 sweep_host.py
Nhập địa chỉ IP hoặc dải mạng (vd: 192.168.110.0/24): 192.168.110.0/24
Dải mạng hợp lệ: 192.168.110.0/24
Các host hoạt động:
Host 192.168.110.0 is up
Host 192.168.110.120 is up
Host 192.168.110.131 is up
Host 192.168.110.2 is up

```

Kết quả khi chạy Nmap:



```
semloh4869@kali: [~/atm]
$ nmap -sn 192.168.110.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-10-21 01:51 PDT
Nmap scan report for 192.168.110.1
Host is up (0.0023s latency).
Nmap scan report for 192.168.110.2
Host is up (0.0019s latency).
Nmap scan report for 192.168.110.129
Host is up (0.000825s latency).
Nmap scan report for 192.168.110.131
Host is up (0.000675s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.63 seconds
semloh4869@kali: [~/atm]
```

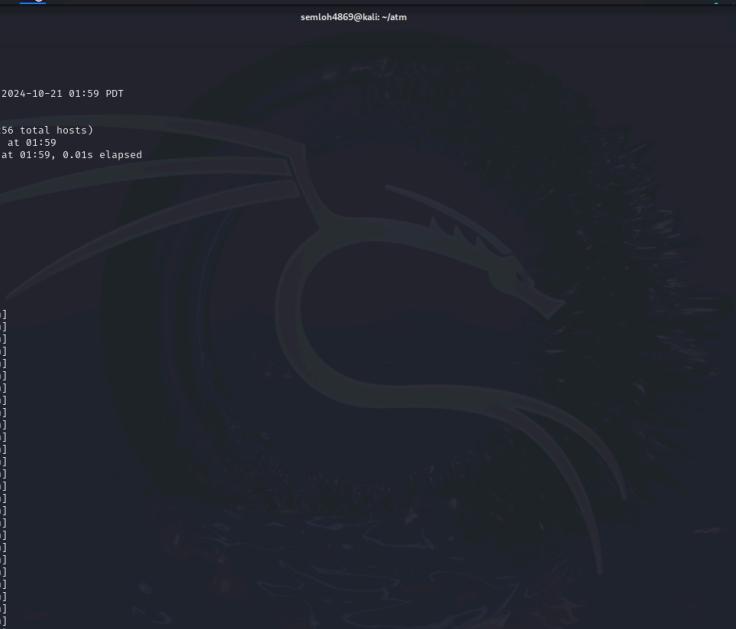
Dựa vào các kết quả trên ta thấy có 4 host đang hoạt động trong mạng.

Câu 33

Tên bài:

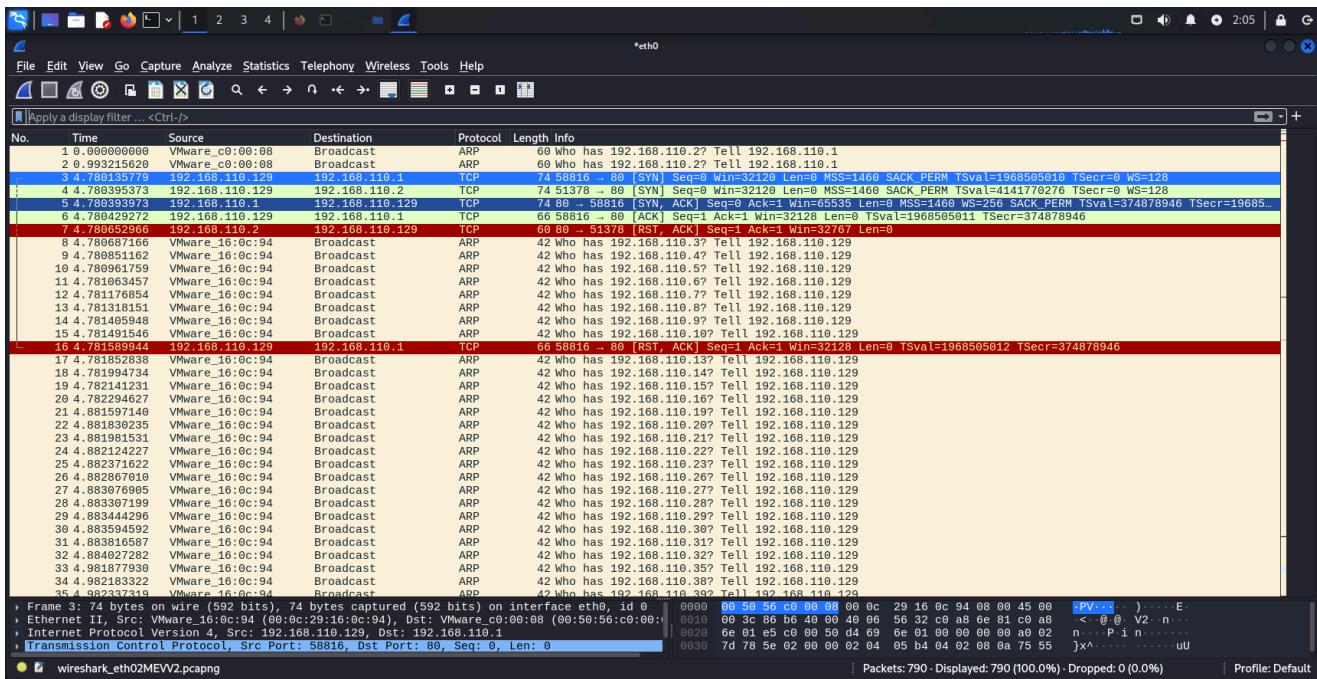
Sử dụng Wireshark để phân tích gói tin khi sử dụng Nmap với tùy chọn -sn

Các bước thực hiện:

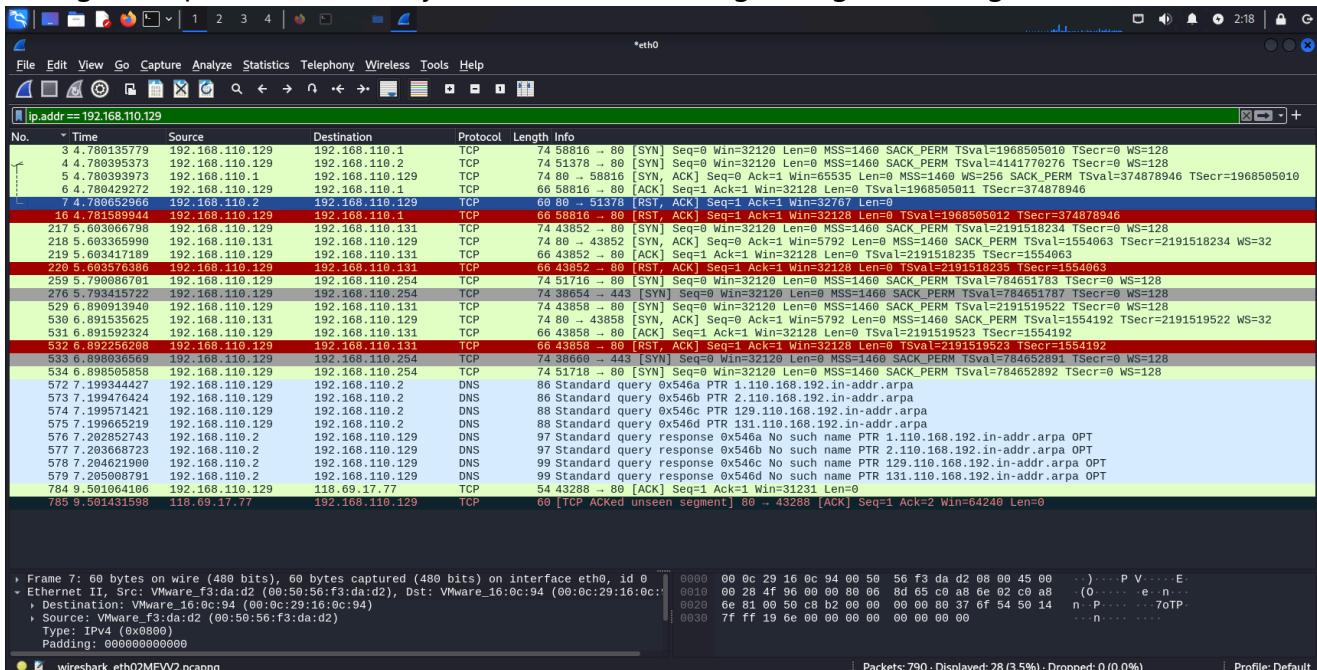


```
semloh4869@kali: [~/atm]
$ nmap -v -sn 192.168.110.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-10-21 01:59 PDT
Initiating Ping Scan at 01:59
Scanning 256 hosts [2 ports/host]
Completed Ping Scan at 01:59, 2.52s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 4 hosts, at 01:59
Completed Parallel DNS resolution of 4 hosts, at 01:59, 0.01s elapsed
Nmap scan report for 192.168.110.0 [host down]
Nmap scan report for 192.168.110.1
Host is up (0.00010s latency).
Nmap scan report for 192.168.110.2
Host is up (0.00010s latency).
Nmap scan report for 192.168.110.3 [host down]
Nmap scan report for 192.168.110.4 [host down]
Nmap scan report for 192.168.110.5 [host down]
Nmap scan report for 192.168.110.6 [host down]
Nmap scan report for 192.168.110.7 [host down]
Nmap scan report for 192.168.110.8 [host down]
Nmap scan report for 192.168.110.9 [host down]
Nmap scan report for 192.168.110.10 [host down]
Nmap scan report for 192.168.110.11 [host down]
Nmap scan report for 192.168.110.12 [host down]
Nmap scan report for 192.168.110.13 [host down]
Nmap scan report for 192.168.110.14 [host down]
Nmap scan report for 192.168.110.15 [host down]
Nmap scan report for 192.168.110.16 [host down]
Nmap scan report for 192.168.110.17 [host down]
Nmap scan report for 192.168.110.18 [host down]
Nmap scan report for 192.168.110.19 [host down]
Nmap scan report for 192.168.110.20 [host down]
Nmap scan report for 192.168.110.21 [host down]
Nmap scan report for 192.168.110.22 [host down]
Nmap scan report for 192.168.110.23 [host down]
Nmap scan report for 192.168.110.24 [host down]
Nmap scan report for 192.168.110.25 [host down]
Nmap scan report for 192.168.110.26 [host down]
Nmap scan report for 192.168.110.27 [host down]
Nmap scan report for 192.168.110.28 [host down]
Nmap scan report for 192.168.110.29 [host down]
Nmap scan report for 192.168.110.30 [host down]
Nmap scan report for 192.168.110.31 [host down]
Nmap scan report for 192.168.110.32 [host down]
Nmap scan report for 192.168.110.33 [host down]
Nmap scan report for 192.168.110.34 [host down]
Nmap scan report for 192.168.110.35 [host down]
Nmap scan report for 192.168.110.36 [host down]
```

Kết quả bắt gói tin trên Wireshark:



Như trong hình ta thấy có rất nhiều gói tin thuộc giao thức ARP được gửi broadcast từ máy ta (192.168.110.129). Nội dung của các gói tin ARP này đều là yêu cầu địa chỉ MAC của các host mà máy ta (192.168.110.129) không xác định được MAC address. Những gói tin này đều không được phản hồi cho thấy các host đó đều đang không hoạt động.



Hình trên thấy các host phản hồi lại máy ta (192.168.110.129) là các host đang hoạt động (192.168.110.1, 192.168.110.2, 192.168.110.131)

Câu 34

Tên bài:

Liệt kê các banner các dịch vụ đang chạy trên máy Metasploitable 2 (Chỉ liệt kê các dịch vụ tcp)

Các bước thực hiện:

Dùng lệnh ip addr để kiểm tra ip của máy Metasploitable 2:

```
msfadmin@metasploitable:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:be:2f:53 brd ff:ff:ff:ff:ff:ff
    inet 192.168.110.131/24 brd 192.168.110.255 scope global eth0
        inet6 fe80::20c:29ff:febe:2f53/64 scope link
            valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:be:2f:5d brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$
```

Địa chỉ ip : 192.168.110.131

Sau đó trên máy kali, ta dùng lệnh nmap để quét và liệt kê các dịch vụ, banner đang chạy trên máy Metasploitable2.

```
(semloh4869㉿kali):~]
Starting Nmap 7.84 ( https://nmap.org ) at 2024-10-21 02:53 PDT
Nmap scan report for 192.168.110.131
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|_  Status:
|   _FTP Server status:
|     Connected to 192.168.110.129
|     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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|_ 1024 60:0:c:f:e:0:5:f:6:a:74:d:9:0:f:a:c:4:d:5:6:c:cd (OSA)
|_ 2048 56:9:6:24:0:f:2:1:1:d:de:a:7:2:a:e:6:1:b:1:24:3:d:e:f:3 (RSA)
23/tcp    open  telnet       telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|_ SSLv2 supported
| ciphers:
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_RC4_40_EXPORT_CBC_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| 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
|_ssl-date: 2024-10-21T09:53:32+00:00; +2s from scanner time.
|_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
```

```
File Actions Edit View Help
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  3          4201/tcp  mountd
|_ 100005  3,2,3     47285/udp mountd
|_ 100021  1,3,4     52892/tcp nllockmgr
|_ 100021  3,4       56508/udp nllockmgr
|_ 100024  1          33806/udp status
|_ 100024  1          58192/tcp 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  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  tcprwapped
1099/tcp  open  java-rmi  GNU Classpath grmregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3380/tcp  open  mysql      MySQL 5.0.51a-3ubuntu5
|_mysql-info:
|_ Protocols: 10
|_ Version: 5.0.51a-3ubuntu5
|_ Thread ID: 9
| Capabilities flags: 43564
| Some Capabilities: LongColumnFlag, SwitchToSSLAfterHandshake, ConnectWithDatabase, SupportsTransactions, Speaks41ProtocolNew, SupportsCompression, Supports41Auth
| Status: Autocommit
|_ SaltedVowdspace1L8\$Si7u
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_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
|_ssl-date: 2024-10-21T09:53:32+00:00; +2s from scanner time.
5900/tcp  open  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
```

```

semloh4869@kali:~$ nmap -A 192.168.110.129
[...]
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: METASPOITABLE
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|   System time: 2024-10-21T05:53:24+00:00
|_ nbstat: NetBIOS name: METASPOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

Clock-skew: mean: 1h00m02s, deviation: 2h00m00s, median: 1s
SMB2-time: Protocol negotiation failed (SMB2)
SMB3-capabilities:
  account_level: guest
  authentication_level: user
  challenge_response: supported
  message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.02 seconds
[semloh4869@kali:~]

```

Câu 35

Tên bài:

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

Các bước thực hiện:

Vào path `/usr/share/nmap/scripts` để chọn NSEscript mong muốn:

```

semloh4869@kali:~$ cd /usr/share/nmap/scripts
[semloh4869@kali:/usr/share/nmap/scripts]$ ls
[...]
acarsd-info.nse      finger.nse          http-svn-info.nse      ms-sql-xp-cmdshell.nse    smb-server-stats.nse
address-info.nse     finger-strings.nse  http-tplink-dir-traversal.nse  msrpc-enum.nse        smb-system-info.nse
afp-brute.nse        firewalk.nse       http-trace.nse        mtrace.nse           smb-vuln-conficker.nse
afp-ls.nse           firewall.nse      http-traceroute.nse  murmur-version.nse  smb-vuln-cve-2017-7494.nse
afp-path-vuln.nse   flume-master-info.nse http-tracepath.nse   mybox.nse            smb-vuln-cve2009-3103.nse
afp-peerdro-nse    foxtail.nse       http-tracepath2.nse  mybox2.nse          smb-vuln-ms07-529.nse
afp-showmount.nse   freelancer.nse   http-tracepath-output.nse mybox-databases.nse  smb-vuln-ms08-067.nse
ajp-auth.nse         ftp-anon.nse      http-useragent-tester.nse mybox-dump-hashes.nse  smb-vuln-ms10-054.nse
ajp-brute.nse       ftp-bounce.nse   http-userdir-enum.nse  mybox-empty-password.nse smb-vuln-ms10-061.nse
ajp-headers.nse    ftp-brute.nse    http-vhosts.nse      mybox-info.nse       smb-vuln-ms17-010.nse
ajp-methods.nse    ftp-bropfite.nse  http-virutotal.nse   mybox-lfi.nse        smb-vuln-regsvc-dos.nse
ajp-request.nse    ftp-proftpd-backdoor.nse http-vlcstreamer-ls.nse mysql-query.nse      smb-vuln-webexec.nse
allseeingeye-info.nse ftp-syst.nse      http-vmware-path-finder.nse mysql-users.nse    smb-webexploit.nse
ampnmap.nse         ftp-wsleakdoor.nse  http-wsleak-nse      mysql-vuln-cve2012-2122.nse smb2-abilities.nse
asn-query.nse       ganglia-info.nse  http-wuln-cve2010-0366.nse mysql-vuln-cve2010-0738.nse  smb2-security-mode.nse
auth-owners.nse    gSOAP.nse        http-wuln-cve2010-2861.nse nat-ppm-info.nse    smb2-time.nse
auth-spoof.nse     gkrellm-info.nse  http-wuln-cve2011-3192.nse nat-ppm-mapport.nse  smb2-vuln-uptime.nse
backorifice-brute.nse gofer-ls.nse    http-wuln-cve2011-3368.nse nbdb-info.nse      smtp-brute.nse
backorifice-info.nse gopher-info.nse  http-wuln-cve2012-1823.nse nbstat.nse        smtp-commands.nse
banner.nse          gpfdl-info.nse  http-wuln-cve2012-8700.nse ncpc-enum-users.nse  smb-enum-users.nse
bittorrent-addr.nse hadoop-data-node-info.nse http-wuln-cve2013-1780.nse ncpc-enum-processes.nse  smb-hp-enum-users.nse
bitcoin-addr.nse    hadoop-mapreduce-info.nse http-wuln-cve2013-1781.nse ncpc-enum-services.nse  smb-ntp-relay.nse
bitcoin-info.nse    hadoop-namenode-info.nse http-wuln-cve2013-7091.nse ndmp-fs-info.nse    smb-ntp-relay.nse
bitcoincrp-info.nse hadoop-secondary-namenode-info.nse http-wuln-cve2014-2126.nse ndmp-version.nse  smb-strangeport.nse
bittorrent-discovery.nse hadoop-tasktracker-info.nse http-wuln-cve2014-2127.nse nessus-brute.nse   smt0-vuln-cve2010-4344.nse
bjnp-discover.nse   hbase-master-info.nse  http-wuln-cve2014-2128.nse nessus-xmrlpc-brute.nse  smt0-vuln-cve2011-1720.nse
broadcast-ataoe-discover.nse hbase-region-info.nse http-wuln-cve2014-2129.nse netbus-auth-bypass.nse  smt0-vuln-cve2011-1764.nse
broadcast-avahi-discover.nse hddtemp-info.nse   http-wuln-cve2014-3704.nse netbus-brute.nse    sniffer-detect.nse
broadcast-bash-discover.nse hmap-info.nse      http-wuln-cve2015-8940.nse netbus-info.nse     smnp-brute.nse
broadcast-bash-discover.nse hostapd-info.nse  http-wuln-cve2015-8941.nse netbus-version.nse  smnp-hp-enum-users.nse
broadcast-dhcp-discover.nse hostapd-kernel.nse http-wuln-cve2015-1625.nse noname-brute.nse  smnp-enum-info.nse
broadcast-dhcp-discover.nse hostapd-krtsh.nse  http-wuln-cve2017-100100.nse nfts-ls.nse       smnp-interfaces.nse
broadcast-dns-service-discovery.nse http-adobe-coldfusion-apache1301.nse http-wuln-cve2017-5638.nse  nfts-stats.nse    smnp-ios-config.nse
broadcast-dropbox-listener.nse http-affiliate-id.nse  http-wuln-cve2017-5689.nse  nfts-showmount.nse  smnp-netstat.nse
broadcast-eigrp-discovery.nse http-apache-negotiation.nse http-wuln-cve2017-8917.nse  nje-node-brute.nse  smnp-processes.nse
broadcast-hid-discoveryd.nse http-apache-server-status.nse http-wuln-misfortune-cookie.nse  nje-pass-brute.nse  smnp-sysdescr.nse
broadcast-igmp-discovery.nse http-aspnets-debug.nse   http-wuln-wnr1000-creds.nse  nntp-ntlm-info.nse  smnp-win32-services.nse
broadcast-igmp-discovery.nse http-ftp-fingerprint.nse http-wuln-wnr1000-creds.nse  nntp-enum.nse     smnp-win32-enum.nse
broadcast-listener.nse   http-auth.nse       http-wuln-wnr1000-creds.nse  ntppe-ehum.nse    smnp-win32-software.nse
broadcast-ms-sql-discover.nse http-avaya-ipoffice-users.nse http-webdav-scan.nse   ntp-info.nse     smnp-win32-users.nse
broadcast-netbios-master-browser.nse http-awstatstotals-exec.nse  http-wordpress-brute.nse  ntp-monlist.nse  socks-auth-info.nse
broadcast-networker-discover.nse http-axis2-dir-traversal.nse http-wordpress-enum.nse  omp2-brute.nse

```

Kết quả sử dụng script "default and safe":

```
semloh4869@kali:[/usr/share/nmap/scripts]
└─# sudo nmap -v 192.168.110.131 --script "default and safe"
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 03:03 PDT
Nmap scan report for 192.168.110.131
Host is up (0.00095s 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 192.168.110.129
|   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 09:0f:cfc:81:c0:5f:6a:74:d6:9b:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:74:9f: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, 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
|_ssl-ciphers:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ssl-date: 2024-10-21T0:04:46+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
80/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
|   100004  2,3,4     2049/udp nfs
|   100005  1,2,3     44814/tcp  mountd
|   100021  1,3,4     52802/tcp  nlockmgr
|   100021  1,3,4     56508/udp nlockmgr
|   100024  1          33806/udp  status
|   100024  1          58192/tcp  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
33806/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 17
|   Capabilities flags: 43564
|   Some Capabilities: Speaks41ProtocolNew, SupportsTransactions, Support41Auth, SupportsCompression, SwitchToSSLAfterHandshake, ConnectWithDatabase, LongColumnFlag
|   Status: Normal
|   Ssl: WO/dn=sEBDnZ:0i:-JR-
5632/tcp  open  postgresql
| 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
|_ssl-date: 2024-10-21T0:04:46+00:00; +3s from scanner time.
5900/tcp  open  vnc
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|     VNC Authentication (2)
6000/tcp  open  X11
6667/tcp  open  irc
| irc-info:
|   users: 1
```

```
semloh4869@kali:[/usr/share/nmap/scripts]
└─# sudo nmap -v 192.168.110.131 --script "default and safe"
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 03:06 PDT
Nmap scan report for 192.168.110.131
Host is up (0.00095s 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 192.168.110.129
|   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 09:0f:cfc:81:c0:5f:6a:74:d6:9b:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:74:9f: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, 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
|_ssl-ciphers:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ssl-date: 2024-10-21T0:04:46+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
80/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
|   100004  2,3,4     2049/udp nfs
|   100005  1,2,3     44814/tcp  mountd
|   100021  1,3,4     52802/tcp  nlockmgr
|   100021  1,3,4     56508/udp nlockmgr
|   100024  1          33806/udp  status
|   100024  1          58192/tcp  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
33806/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 17
|   Capabilities flags: 43564
|   Some Capabilities: Speaks41ProtocolNew, SupportsTransactions, Support41Auth, SupportsCompression, SwitchToSSLAfterHandshake, ConnectWithDatabase, LongColumnFlag
|   Status: Normal
|   Ssl: WO/dn=sEBDnZ:0i:-JR-
5632/tcp  open  postgresql
| 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
|_ssl-date: 2024-10-21T0:04:46+00:00; +3s from scanner time.
5900/tcp  open  vnc
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|     VNC Authentication (2)
6000/tcp  open  X11
6667/tcp  open  irc
| irc-info:
|   users: 1
```

```

semloh4869@kali: /usr/share/nmap/scripts
File Actions Edit View Help
|_ .Not valid after: 2010-04-16T14:07:45
|_ _ssl-date: 2024-10-21T10:04:46+00:00; +3s from scanner time.
5900/tcp open  vnc
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|     Unauthenticated (2)
6000/tcp open  X11
6667/tcp open  irc
| 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, 0:14:14
|   source ident: nmap
|   source host: 81660C73.7678D100.FFFA6D49.IP
|_ error: Closing Link: fxdzprnxz[192.168.110.129] (Quit: fxdzprnxz)
8009/tcp open  ajp13
|_ajp13-methods: Failed to get a valid response for the OPTION request
8100/tcp open  unknown
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/7.5
MAC Address: 00:0C:29:BE:2F:53 (VMware)

Host script results:
| smb-os-discovery:
|   OS: Linux (SUSE Linux Enterprise Server 3.0-20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2024-10-21T06:03:35-04:00
|_clock-skew: mean: 1h00m02s, deviation: 2h00m00s, median: 2s
| smb-security-mode:
|_ security-mode: blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)

Nmap done: 1 IP address (1 host up) scanned in 71.64 seconds
[semloh4869@kali]-[/usr/share/nmap/scripts]

```

Kết quả sử dụng script `firewall-bypass`:

```

semloh4869@kali: /usr/share/nmap/scripts
File Actions Edit View Help
domcon-cmd.nse          http-robtex-shared.nse          mrinfo.nse           smb-enum-sessions.nse      whois-ip.nse
domino-enum-users.nse    http-sap-newweaver-leak.nse  ms-sql-brute.nse    smb-enum-shares.nse       wsdd-discover.nse
dpaq-brute.nse          http-security-headers.nse  ms-sql-config.nse   smb-enum-users.nse       x11-access.nse
drcd-enum.nse           http-slowloris-nse          ms-sql-dump.nse     smb-flood.nse          xodbc-poc.nse
drda-Info.nse           http-shellshock.nse        ms-sql-dump-hashes.nse  smb-fuzz.nse          xmrig-l-methods.nse
duplicates.nse          http-sitemap-generator.nse  ms-sql-empty-password.nse  smb-enum, nse         xmpp-brute.nse
eap-info.nse            http-slowloris-check.nse   ms-sql-hasdbaccess.nse  smb-discovery.nse      xmpp-info.nse
enip-info.nse           http-slowloris.nse        ms-sql-injection.nse   smb-print-text.nse
epmd-info.nse           http-sql-stored-xss.nse    ms-sql-html-info.nse   smb-protocols.nse
epcc-enum-processes.nse http-stored-xss.nse        ms-sql-query.nse     smb-psexec.nse
fcrdns.nse              http-svn-enum.nse        ms-sql-tables.nse    smb-security-mode.nse

[semloh4869@kali]-[/usr/share/nmap/scripts]
└─$ sudo nmap 192.168.110.131 -script "firewall-bypass.nse"
Starting Nmap 7.94SYN ( https://nmap.org ) at 2024-10-21 03:09 PDT
Nmap scan report for 192.168.110.131
Host is up (0.001s 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
2181/tcp  open  ccproxy-ftp
3300/tcp  open  mysql
5422/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:BE:2F:53 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.95 seconds
[semloh4869@kali]-[/usr/share/nmap/scripts]

```