

BÁO CÁO THỰC HÀNH

Môn học: NT140.P12.ANTT – An Toàn Mạng

Tên chủ đề: Lab 3 - Gather information & Vulnerability Scanning

GVHD: Tô Trọng Nghĩa

Nhóm: 6

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT140.P12.ANTT.2

STT	Họ và tên	MSSV	Email
1	Lại Quan Thiên	22521385	22521385@gm.uit.edu.vn
2	Mai Nguyễn Nam Phương	22521164	22521164@gm.uit.edu.vn
3	Hồ Diệp Huy	22520541	22520541@gm.uit.edu.vn
4	Đặng Đức Tài	22521270	22521270@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:

STT	Nội dung	Tình trạng	Thực hiện
1	Task 1	100%	Đức Tài
2	Task 2	100%	Quan Thiên
3	Task 3	100%	Diệp Huy
4	Task 4	100%	Diệp Huy
5	Task 5	100%	Quan Thiên
6	Task 6	100%	Nam Phương
7	Task 7	100%	Đức Tài
8	Task 8	100%	Đức Tài
9	Task 9	100%	Đức Tài
10	Task 10	100%	Quan Thiên
11	Task 11	100%	Nam Phương
12	Task 12	100%	Diệp Huy
13	Task 13	100%	Nam Phương
14	Task 14	100%	Diệp Huy
15	Task 15	100%	Quan Thiên
16	Task 16	100%	Nam Phương
Điểm tự đánh giá			10/10

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

BÁO CÁO CHI TIẾT

Task 1: Thực hiện truy cập vào website của MegaCorp One tại (<https://www.megacorpone.com/>) và trả lời các câu hỏi sau:

- Tìm trang web của MegaCorp One, hãy mô tả một chút về lĩnh vực hoạt động của công ty?
- Hãy liệt kê những thành viên đang làm việc cho MegaCorp One và một vài thông tin về những thành viên đó (địa chỉ email, chức vụ, tài khoản mạng xã hội)?
- Khi có được địa chỉ Email của các thành viên thuộc tổ chức, bạn có phát hiện ra điều gì?

Trả lời:

MegaCorp One hoạt động trong lĩnh vực công nghệ nano với mục tiêu dẫn đầu trong đổi mới sáng tạo và tạo ra công nghệ tiên tiến. Công ty chuyên cung cấp các sản phẩm và dịch vụ ứng dụng công nghệ nano trong y học, quốc phòng, và các lĩnh vực thương mại. Các dịch vụ nổi bật bao gồm:

- Tái tạo tế bào.
- Hệ thống bồi sung miễn dịch.
- Sửa chữa bằng micromachine.
- Vũ khí nano.
- Hệ thống đồng hóa thực thể bằng nanobot.

Các thành viên trong công ty và thông tin chi tiết:

HỌ TÊN	CHỨC VỤ	EMAIL	TWITTER
Joe Sheer	CEO	joe@megacorpone.com	@Joe_Sheer
Tom Hudson	Web Designer	thudson@megacorpone.com	@TomHudsonMCO
Tanya Rivera	Senior Developer	trivera@megacorpone.com	@TanyaRiveraMCO
Matt Smith	Marketing Director	msmith@megacorpone.com	@MattSmithMCO
Mike Carlow	VP of Legal	mcarlow@megacorpone.com	Không có thông tin
Alan Grofield	IT and Security Director	agrofield@megacorpone.com	Không có thông tin

Nhận xét về các địa chỉ email:

- Cấu trúc nhất quán: Các địa chỉ email của nhân viên MegaCorp One sử dụng định dạng `tendau@megacorpone.com`. Đây là một chuẩn mực phổ biến và có thể sử dụng để dự đoán các email khác chưa được liệt kê.

- Nguy cơ tấn công: Những email này có thể được khai thác cho các cuộc tấn công phishing hoặc brute force nếu không được bảo vệ đúng cách.
- Đặc điểm tổ chức: Email cho các phòng ban như Human Resources (hr@megacorpone.com) hoặc Sales (sales@megacorpone.com) cũng tuân theo định dạng tương tự, cho thấy hệ thống email được chuẩn hóa theo chức năng.

Thông tin này hữu ích để tiếp tục điều tra trong các kịch bản an ninh mạng thực tế hoặc thử nghiệm an toàn.

Task 2: Sử dụng công cụ whois trả lời các câu hỏi sau:

- Xác định các name server của MegaCorp One.
- Có thể tìm kiếm các thông tin của trường Đại học Công nghệ Thông tin (uit.edu.vn) có được không? Giải thích?
- Thu thập thông tin về tên miền uit.edu.vn và hãy cho biết các thông tin như: Ngày đăng ký tên miền, Ngày hết hạn tên miền, Chủ sở hữu tên miền, Các name server của tên miền?

Trả lời:

- Xác định các name server của MegaCorp One:** Các name server của MegaCorp One là:
 - NS1.MEGACORPONE.COM
 - NS2.MEGACORPONE.COM
 - NS3.MEGACORPONE.COM

- Có thể tìm kiếm các thông tin của trường Đại học Công nghệ Thông tin (uit.edu.vn) có được không? Giải thích:**

Hiện tại không thể tìm kiếm các thông tin của tên miền uit.edu.vn bằng công cụ whois. Tên miền ".vn" không có máy chủ whois công khai giống như các tên miền quốc tế (.com, .net) mà thay vào đó, thông tin được quản lý bởi VNNIC (Trung tâm Internet Việt Nam). Để tra cứu thông tin chi tiết về tên miền uit.edu.vn, ta có thể truy cập trực tiếp vào trang web của VNNIC tại <http://www.vnnic.vn/en>.

- Thông tin về tên miền uit.edu.vn:**

Để thu thập thông tin cụ thể về uit.edu.vn, ta cần truy vấn whois cho tên miền này trên <http://www.vnnic.vn/en>. Thông tin sẽ bao gồm:

- Ngày đăng ký tên miền và Ngày hết hạn tên miền
- Chủ sở hữu tên miền
- Các name server

The screenshot shows the homepage of the Vietnam Internet Network Information Center (VNNIC). The header includes the VNNIC logo, the text "Internet for all", and the full name "MINISTRY OF INFORMATION AND COMMUNICATIONS VIETNAM INTERNET NETWORK INFORMATION CENTER". A search bar and social media links are also present. Below the header is a navigation menu with links to "HOME", "INTERNET RESOURCES", "INTERNET INFRASTRUCTURE", "STATISTICS", and "ABOUT". The main content area is titled "VNNIC INTERNET RESOURCE WHOIS INFORMATION". It displays the following WHOIS data:

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:	2029-10-02
Status:	clientTransferProhibited
Nameserver:	ns1.pavietnam.vn ns2.pavietnam.vn nsbak.pavietnam.net
DNSSEC:	unsigned

Task 3: Trả lời các câu hỏi sau:

- Ai là Phó chủ tịch Pháp lý (Vice President of Legal) của MegaCorp One và địa chỉ email của họ là gì?
- Bạn có thể tìm kiếm thêm các nhân viên khác của MegaCorp One mà không được liệt kê trên trang web www.megacorpone.com?
- Liệt kê một vài từ khóa thường gặp trên Google và cho ví dụ? (Yêu cầu: ít nhất 5 từ khóa)
- Thực hiện tìm kiếm các tài liệu thú vị của Trường Đại học Công nghệ Thông tin mà được công bố trên Internet mà bạn là không nên được công bố?

Trả lời:

- a. Ai là Phó chủ tịch Pháp lý (Vice President of Legal) của MegaCorp One và địa chỉ email của họ là gì?

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

Khoảng 13.600 kết quả (0,26 giây)

Mike Carlow - VP of Legal Affairs - MegaCorp One | LinkedIn.

linkedin.com
https://www.linkedin.com › ...

Mike Carlow - VP of Legal Affairs - MegaCorp One - LinkedIn

Giới thiệu về đoạn trích nổi bật · Phản hồi

Mọi người cũng hỏi :

What is Megacorpone?

Phản hồi

megacorpone.com
https://www.megacorpone.com › contact

Contact Us - MegaCorp One

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

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

- Tìm kiếm trên LinkedIn: site:linkedin.com “MegaCorp One”

The screenshot shows a LinkedIn search interface with the query "MegaCorp One". It displays four search results:

- Mutunga Muli**
Electrical Specialist at MegaCorp One
Nairobi County, Kenya · [Contact info](#)
Connect Message More
- Vicuong Ha**
Manager at MegaCorp One
Vietnam · [View](#)
- Emac Oscp**
Senior Tester at MegaCorp One
Deadwood, SD, US · [View](#)
- Ga Rod**
Boss at MegaCorp One
Panama City Beach, FL, US · [View](#)

Each profile card includes a "View" button to the right.

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

- site

site:wikipedia.org: Giới hạn kết quả tìm kiếm cho một trang web hoặc một tên miền cụ thể

Google search results for "site:wikipedia.org". The results show two Wikipedia pages:

- Work with us - Wikimedia Foundation**
The Wikimedia Foundation is looking for an enterprising lead product manager to coordinate our efforts in artificial intelligence and machine learning, all ...
- Area codes 314 and 557**
Area codes 314 and 557 are telephone area codes in the North American Numbering Plan (NANP) in the U.S. state of Missouri, serving the city of St. Louis and ...

- filetype

filetype:pdf Tìm kiếm các tệp tin có định dạng cụ thể

Google search results for "an toàn mạng filetype:pdf". The results show three PDF files:

- AN TOÀN MẠNG MÁY TÍNH - Feuer.vn**
An ninh **mạng** là một thành phần chủ yếu của an ninh thông tin. Ngoài an ninh **mạng**, an ninh thông tin còn có mối quan hệ với một số lãnh vực an ninh khác, bao ...
66 trang
- Cẩm nang An toàn trực tuyến**
Cẩm nang "An toàn trực tuyến" được cung cấp bởi Cục An toàn thông tin (Bộ Thông tin và Truyền thông) phối hợp cùng Google biên soạn, sẽ đưa ra những hướng dẫn ...
41 trang
- hướng dẫn đảm bảo an toàn thông tin, tham gia môi ...**
Mục đích cơ bản của an ninh **mạng** là giữ **an toàn** cho người dùng và dữ liệu. Theo nguyên tắc truyền



- inurl

inurl:signup Tìm kiếm các trang có chứa từ khóa trong URL của trang web.

Google search results for "inurl:signup":

- SignUp.com Mobile**
We handle the busy work, so you can enjoy the moments. Easily create free online Signup sheets, manage volunteer scheduling, and more!
[Find My SignUp](#) · [Plans & Pricing](#) · [Register](#) · [Team SignUp.com](#)
- Find my current SignUp sheet**
Login My SignUps Try a Demo Become an Organizer. Visit Desktop Version. MENU. Dashboard; My Spots; My Info; Location; Contact Organizer; Swap on Desktop ...
- Microsoft**
https://signup.live.com · Dịch trang này

- intext

intext:facebook Tìm kiếm các trang có chứa từ khóa trong nội dung của trang web

Google search results for "intext:facebook":

- Facebook - Ứng dụng trên Google Play**
Nơi người thật thổi bùng sự hiếu kỳ trong bạn. Dù bạn đang bán đồ cũ, hiển thị thước phim cho nhóm người muốn xem hay chia sẻ tiếng cười qua những hình ảnh ...
4,5 ★★★★★ (156.065.160) · Miễn phí · Android · Mạng xã hội
- Facebook – Wikipedia tiếng Việt**
Facebook là phương tiện truyền thông xã hội và dịch vụ mạng xã hội trực tuyến thành lập vào năm 2004 của Mỹ thuộc sở hữu của Meta Platforms có trụ sở tại ...
- Facebook trên App Store - Apple**
Nơi người thật thổi bùng sự hiếu kỳ trong bạn. Dù bạn đang bán đồ cũ, hiển thị thước phim cho nhóm người muốn xem hay chia sẻ tiếng cười qua những hình ảnh ...
4,4 ★★★★★ (4.194.868) · Miễn phí · iOS
- Tin tức, Video, hình ảnh Facebook**
Facebook: Tất cả thông tin mới nhất, video clip và hình ảnh về Facebook trên CafeBiz.

Andrew McCollum, Chris Hughes
Giá cổ phiếu: META (NASDAQ)
554,08 US\$ -23,08 (-4,00%)
16:00 EST 15 thg 11 - Tuyên bố từ chối trách nhiệm

Công ty con: WhatsApp, Reality Labs, Công nghệ Meta Platforms · Xem thêm

Ngày thành lập: tháng 2 năm 2004, Cambridge, Massachusetts, Hoa Kỳ

Trụ sở: Menlo Park, California, Hoa Kỳ
Tuyên bố từ chối trách nhiệm

Mọi người cũng tìm kiếm

Instagram LinkedIn Facebook

Ý kiến phản hồi



- intitle

intitle:basic Tìm kiếm các trang có chứa từ khóa trong tiêu đề của trang web

BASIC được phát minh vào năm 1963 bởi các giáo sư John ...

BASIC VIETNAM - Thiết Bị Vệ Sinh Chăm Sóc
Thiết bị vệ sinh chăm sóc Basic Việt Nam chuyên cung cấp các thiết bị cho nhà vệ sinh như bồn cầu chăm sóc, bồn cầu thông minh, lavabo, vòi chậu, vòi rửa, ...

basic – Wiktionary tiếng Việt
basic /'ber.sɪk/. Cơ bản, cơ sở. basic principle — những nguyên tắc cơ bản: basic frequency — tần số cơ sở. (Hoá học) (thuộc) bazo.

BASIC
Các sản phẩm trong Bộ sưu tập này mang màu sắc trung tính, có tính ứng dụng cao phù hợp với nhiều địa điểm, nhiều dáng người, tôn đường nét mềm mại, nữ tính ...

Basic

d. 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?

- Vào uit.edu.vn → Tra cứu: tìm được danh sách thí sinh đăng ký tham gia kỳ thi tuyển sinh trình độ thạc sĩ, gồm mssv và các thông tin cá nhân

HỘ ĐỒNG TSSDH NĂM 2024 DANH SÁCH THÍ SINH ĐĂNG KÝ THAM GIA KỲ THI TUYỂN SINH TRÌNH ĐỘ THẠC SĨ KHÓA 19-DQT 2-NĂM 2024										
TT	Số HS	HỌ VÀ TÊN	Giới	NGÀY SINH	NƠI SINH	Ngành DKDT	BTKT	Lý do miễn AV	Hình thức	
1	S24-2-001	Trần Lâm Hải	An	Nam	02-07-1994	Vĩnh Long	KTMT		Xét tuyển đánh giá hồ sơ+ phỏng vấn chuyên môn	
2	S24-2-120	Âu Hồng	Ân	Nam	17-05-1989	TPHCM	KHMT	VSTEP B1 Trường ĐH KHIXINV 19/12/2023	Xét tuyển đánh giá hồ sơ+ phỏng vấn chuyên môn	
3	S24-2-002	Trần Bảo	Ân	Nữ	20-08-2001	Trà Vinh	HTTT		Xét tuyển đánh giá hồ sơ	
4	S24-2-003	Lý Hồng Thiên	Ân	Nữ	01-08-1999	An Giang	HTTT	HSK 3 28/01/2024	Xét tuyển đánh giá hồ sơ	
5	S24-2-004	Nguyễn Văn	Anh	Nữ	15-04-2002	TPHCM	KHMT	JLPT N3 11/01/2024	Xét tuyển thẳng	
6	S24-2-005	Lê	Anh	Nam	19-04-2002	Bạc Liêu	KHMT	VSTEP B1 Trường ĐH KT-TC TPHCM 09/4/2024	Xét tuyển thẳng	
7	S24-2-006	Nguyễn Thị Hoàng	Anh	Nữ	29-05-2002	An Giang	CNTT	IELTS 5.0 29/4/2021 xét TNĐH	Xét tuyển thẳng	

Page 1

- Ngoài ra, ta gõ: **site:uit.edu.vn @gm.uit.edu.vn** vào google.com. Thấy được rất nhiều trang lô được địa chỉ email sinh viên UIT, trong đó có 1 Sheet của google không giới hạn quyền truy cập “chỉ sinh viên hoặc cán bộ/nhân viên UIT”, mà cấp cho tất cả mọi người, dẫn đến lộ 1070 địa chỉ Email sinh viên UIT Khoa 2017.

The screenshot shows a Google search result for the query "site:uit.edu.vn @gm.uit.edu.vn". The top result is a link to a Google Sheets document titled "Untitled Spreadsheet - Cảng thông tin đào tạo". This document contains a table with student information, including names like Lê Hoàng Anh, Nguyễn Văn Phương, and others, along with their corresponding emails and scores. The entire document is highlighted with a red box.

The screenshot shows the Google Sheets document "danh_sach_xep_lop_anh_van.xlsx" opened in Microsoft Edge. The document is titled "DANH SÁCH XẾP LỚP ANH VĂN KHÓA 2017" and lists 15 students with their names, scores, and grades. The columns are labeled STT, Mã số sinh viên/Họ, Tên, Email, Điểm / 100, Xếp vào lớp, and Ghép ché. The data is as follows:

STT	Mã số sinh viên/Họ	Tên	Email	Điểm / 100	Xếp vào lớp	Ghép ché
1	17520958	Liên Hiệp	Quốc	96	Anh văn 3	
2	17520208	Lê Hoàng	An	95	Anh văn 2	
3	17520247	Nguyễn Văn Phương	Anh	95	Anh văn 2	
4	17520563	Bùi Đăng	Huy	95	Anh văn 2	
5	17521122	Hà Quốc	Tiến	95	Anh văn 2	
6	17521305	Trần Hoàng	Long	95	Anh văn 2	
7	17520805	Vũ Đình Vĩ	Nghiêm	94	Anh văn 2	
8	17520860	Phạm Thúy	Nhung	94	Anh văn 2	
9	17521113	Võ Thành	Thuần	94	Anh văn 2	
10	17520206	Hồ Thái	An	93	Anh văn 2	
11	17520323	Nguyễn Thành	Danh	93	Anh văn 2	
12	17520755	Nguyễn Duy	Minh	93	Anh văn 2	
13	17520793	Lê Thành	Nghị	93	Anh văn 2	
14	17520976	Nguyễn Quốc Nam	Sang	93	Anh văn 2	
15	17521199	Nouyenv Doan Anh	Tú	93	Anh văn 2	

STT	Mã số sinh viên	Họ	Tên	Email	Điểm /100	Xếp vào lớp	Ghi chú
8	17520958	Liên Hiệp	Quốc	17520958@gm.uit.edu.vn	96	Anh văn 3	
9	17520208	Lê Hoài	Ân	17520208@gm.uit.edu.vn	95	Anh văn 2	
10	17520247	Nguyễn Văn Phượng	Anh	17520247@gm.uit.edu.vn	95	Anh văn 2	
11	17520563	Bùi Đăng	Huy	17520563@gm.uit.edu.vn	95	Anh văn 2	
12	17521122	Hà Quốc	Tiến	17521122@gm.uit.edu.vn	95	Anh văn 2	
13	17521305	Trần Hoàng	Long	17521305@gm.uit.edu.vn	95	Anh văn 2	
14	17520805	Vũ Dinh Vĩ	Nghiem	17520805@gm.uit.edu.vn	94	Anh văn 2	
15	17520860	Phạm Thúy	Nhung	17520860@gm.uit.edu.vn	94	Anh văn 2	
16	17521113	Võ Thành	Thuần	17521113@gm.uit.edu.vn	94	Anh văn 2	
17	17520206	Hồ Thái	An	17520206@gm.uit.edu.vn	93	Anh văn 2	
18	17520323	Nguyễn Thành	Danh	17520323@gm.uit.edu.vn	93	Anh văn 2	
19	17520755	Nguyễn Duy	Minh	17520755@gm.uit.edu.vn	93	Anh văn 2	
20	17520793	Lê Thành	Nghi	17520793@gm.uit.edu.vn	93	Anh văn 2	
21	17520976	Nguyễn Quốc Nam	Sang	17520976@gm.uit.edu.vn	93	Anh văn 2	
22	17521199	Nguyễn Đoàn Anh	Tú	17521199@gm.uit.edu.vn	93	Anh văn 2	
23	17520604	Lưu Quang	Khai	17520604@gm.uit.edu.vn	92	Anh văn 2	
24	17520261	Lê Việt	Bách	17520261@gm.uit.edu.vn	91	Anh văn 2	

Task 4: Sử dụng Netcraft để xác định máy chủ ứng dụng (application server) đang chạy trên www.megacorpone.com

Trả lời:

- Truy cập <https://searchdns.netcraft.com/> → Resources → Research Tools → Sitereport
- Trong thanh tìm kiếm nhập [https://www.megacorpone.com/](http://www.megacorpone.com/), thu được các kết quả:

Background

Site title: MegaCorp One - Nanotechnology Is the Future Date first seen: December 2018

Site rank: 49405 Primary language: English

Description: Not Present

Network

Site: https://www.megacorpone.com Domain: megacorpone.com
Netblock Owner: OVH Hosting, Inc. Nameserver: ns1.megacorpone.com
Hosting company: OVH Domain registrar: gandi.net
Hosting country: CA Nameserver organisation: whois.gandi.net
IPv4 address: 149.56.244.87 (Whoisfeel ID: A518276) Organisation: MegaCorpOne, Rachel, 89001, United States
IPv4 autonomous systems: AS16276 DNS admin: admin@megacorpone.com
IPv6 address: Not Present Top Level Domain: Commercial entities (.com)
IPv6 autonomous systems: Not Present DNS Security Extensions: Enabled
Reverse DNS: www.megacorpone.com

IP delegation

IPv4 address (149.56.244.87)

IP range	Country	Name	Description
::ffff:0,0,0,0/96	United States	[IANA-IPv4-MAPPED-ADDRESS]	Internet Assigned Numbers Authority
↳ 149.0.0.0-149.255.255	United States	NET149	Various Registries (Maintained by ARIN)
↳ 149.56.0.0-149.56.255.255	Canada	HD-2	OVH Hosting, Inc.
↳ 149.56.244.0-149.56.244.255	Canada	OVH-DEDICATED-FO	OVH Hosting, Inc.
↳ 149.56.244.87	Canada	OVH-DEDICATED-FO	OVH Hosting, Inc.

- Nhận thấy, máy chủ ứng dụng đang chạy trên megacorpone.com là Apache.

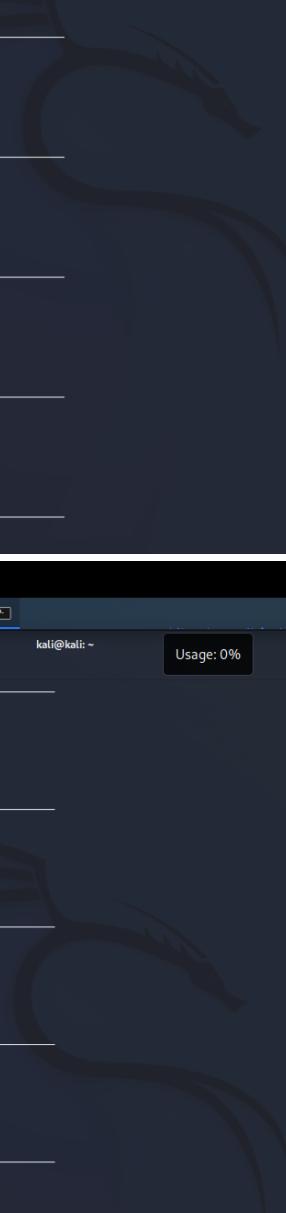
Task 5:

- a. Thực hiện sử dụng module có thể giúp phân giải tên miền ở Hình thành địa chỉ IP tương ứng.
 - b. Sử dụng một số module khác có trong recon-ng để thu thập thông tin về UIT nhiều nhất có thể.

Trả lời:

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

- Sử dụng recon/domains-hosts/hackertarget để phân giải.



```

[+] Kali Linux 2022 x
File Actions Edit View Help
[recon-ng][default] > modules load recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > options set SOURCE megacorpone.com
SOURCE => megacorpone.com
[recon-ng][default][hackertarget] > run

MEGACORPONE.COM
[*] Country: None
[*] Host: admin.megacorpone.com
[*] Ip_Address: 51.222.169.208
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: beta.megacorpone.com
[*] Ip_Address: 51.222.169.209
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: fsi.megacorpone.com
[*] Ip_Address: 51.222.169.210
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: intranet.megacorpone.com
[*] Ip_Address: 51.222.169.211
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: mail.megacorpone.com
[*] Ip_Address: 51.222.169.212
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: mail2.megacorpone.com
[*] Ip_Address: 51.222.169.213
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: ns1.megacorpone.com
[*] Ip_Address: 51.79.37.18
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: ns2.megacorpone.com
[*] Ip_Address: 51.222.39.63
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: ns3.megacorpone.com
[*] Ip_Address: 66.70.207.180
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: router.megacorpone.com
[*] Ip_Address: 51.222.169.214
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: siem.megacorpone.com
[*] Ip_Address: 51.222.169.215
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]

```

```

[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: syslog.megacorpone.com
[*] Ip_Address: 51.222.169.217
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: test.megacorpone.com
[*] Ip_Address: 51.222.169.219
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: vpn.megacorpone.com
[*] Ip_Address: 51.222.169.220
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: www.megacorpone.com
[*] Ip_Address: 149.56.244.87
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: www2.megacorpone.com
[*] Ip_Address: 149.56.244.87
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]

SUMMARY

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

- Xem lịch sử các hosts:

```

[*] Country: None
[*] Host: www2.megacorpone.com
[*] Ip_Address: 149.56.244.87
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]

SUMMARY

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

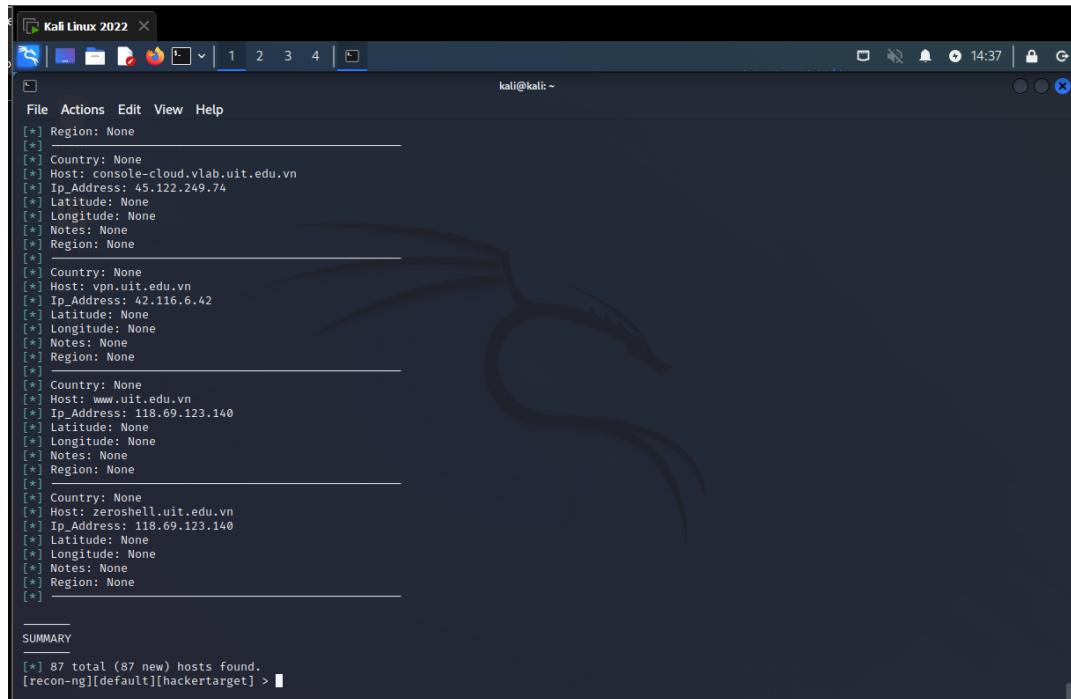
+-----+
| rowid | host | ip_address | region | country | latitude | longitude | notes | module |
+-----+
| 1 | admin.megacorpone.com | 51.222.169.208 | | | | | | hackertarget |
| 2 | beta.megacorpone.com | 51.222.169.209 | | | | | | hackertarget |
| 3 | fs1.megacorpone.com | 51.222.169.210 | | | | |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

[*] 18 rows returned
[recon-ng][default][hackertarget] > 
```

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

Trả lời:

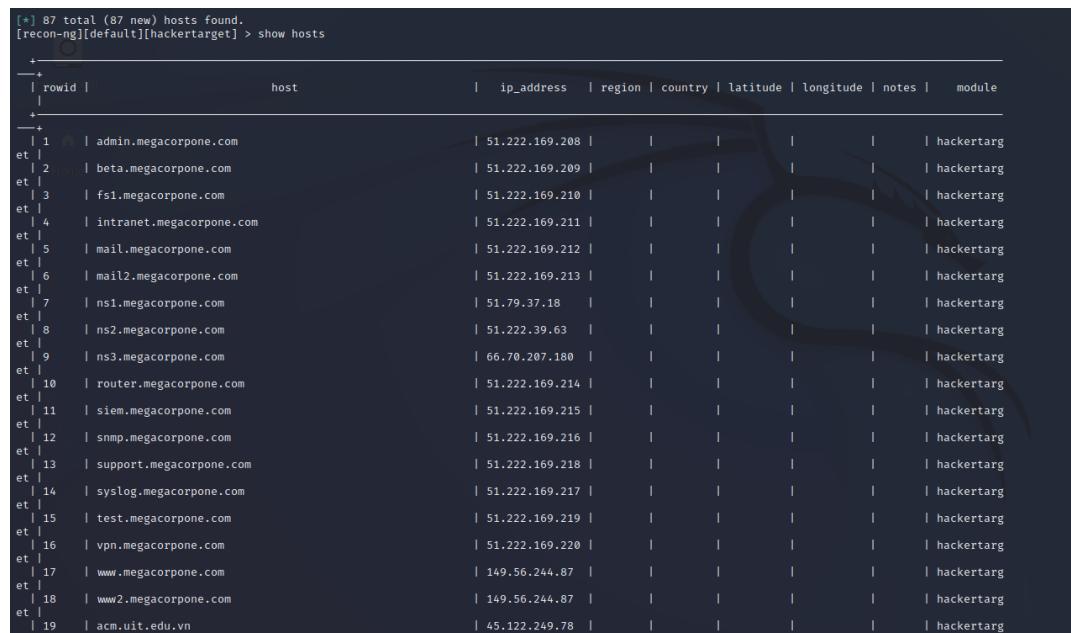
- Tiếp tục sử dụng hackertarget để tìm thông tin về UIT, có 87 host được tìm thấy.



```

[*] Region: None
[*]
[*] Country: None
[*] Host: console-cloud.vlab.uit.edu.vn
[*] Ip_Address: 45.122.249.74
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: vpn.uit.edu.vn
[*] Ip_Address: 42.116.6.42
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: www.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: zeroshell.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] SUMMARY
[*] 87 total (87 new) hosts found.
[recon-ng][default][hackbar] > 

```



```

[*] 87 total (87 new) hosts found.
[recon-ng][default][hackbar] > show hosts
+---+-----+-----+-----+-----+-----+-----+-----+-----+
| rowid | host | ip_address | region | country | latitude | longitude | notes | module |
+---+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin.megacorpone.com | 51.222.169.208 | | | | | | hackertarg
| 2 | beta.megacorpone.com | 51.222.169.209 | | | | | | hackertarg
| 3 | fs1.megacorpone.com | 51.222.169.210 | | | | | | hackertarg
| 4 | intranet.megacorpone.com | 51.222.169.211 | | | | | | hackertarg
| 5 | mail.megacorpone.com | 51.222.169.212 | | | | | | hackertarg
| 6 | mail2.megacorpone.com | 51.222.169.213 | | | | | | hackertarg
| 7 | ns1.megacorpone.com | 51.79.37.18 | | | | | | hackertarg
| 8 | ns2.megacorpone.com | 51.222.39.63 | | | | | | hackertarg
| 9 | ns3.megacorpone.com | 66.70.207.180 | | | | | | hackertarg
| 10 | router.megacorpone.com | 51.222.169.214 | | | | | | hackertarg
| 11 | siem.megacorpone.com | 51.222.169.215 | | | | | | hackertarg
| 12 | snmp.megacorpone.com | 51.222.169.216 | | | | | | hackertarg
| 13 | support.megacorpone.com | 51.222.169.218 | | | | | | hackertarg
| 14 | syslog.megacorpone.com | 51.222.169.217 | | | | | | hackertarg
| 15 | test.megacorpone.com | 51.222.169.219 | | | | | | hackertarg
| 16 | vpn.megacorpone.com | 51.222.169.220 | | | | | | hackertarg
| 17 | www.megacorpone.com | 149.56.244.87 | | | | | | hackertarg
| 18 | www2.megacorpone.com | 149.56.244.87 | | | | | | hackertarg
| 19 | acm.uit.edu.vn | 45.122.249.78 | | | | | | hackertarg

```



```
[*] 105 rows returned
[recon-ng][default][hacket targ] > |
```

Task 6: Sử dụng 1 trong 2 công cụ Gitrob hoặc Gitleaks để tìm kiếm các thông tin nhạy cảm bị rò rỉ đối với các trường đại học thành viên trong ĐHQG

Trả lời:

- Ta sử dụng gitleaks để kiểm tra một repository liên quan đến Front-end của một ứng dụng: [vutuanhai237/FrontendStudyingBoard: Website for Studying board](#)

```
(kali㉿kali)-[~/Downloads/ATM 3]
$ gitleaks detect --source FrontendStudyingBoard/ --report-path /home/kali/Downloads/ATM 3/rp.txt

gitleaks

11:17AM INF 172 commits scanned.
11:17AM INF scan completed in 12.3s
11:17AM WRN leaks found: 1
```

- Có thể thấy ở file báo cáo tâ phát hiện ra được một thông tin nhạy cảm bên trong repo, tiến hành xem xét file report để tìm hiểu rõ hơn về thông tin bị tiết lộ

```
GNU nano 8.1
{
  "Description": "Generic API Key",
  "Startline": 20,
  "Endline": 20,
  "StartColumn": 26,
  "EndColumn": 82,
  "Match": "apiKey=\\"pgsfnb617zvx79gf1fo6sauiik6bg2icroka7q4flelxesr\\\"",
  "Secret": "pgsfnb617zvx79gf1fo6sauiik6bg2icroka7q4flelxesr",
  "File": "src/component/layout/create_post.js",
  "SymlinkToFile": "",
  "Commit": "1a34ee322de8c67ce0569d661464d17690b14f3a",
  "Entropy": 4.4996019,
  "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\ncommit aef7a4860c0a6cb6f14a24b78527884a9f872256\nAuthor: vutuanhai237 \u003c43202025+vutuanhai237@users.noreply.github.com\u003e",
  "Tags": [],
  "RuleID": "generic-api-key",
  "Fingerprint": "1a34ee322de8c67ce0569d661464d17690b14f3a:src/component/layout/create_post.js:generic-api-key:20"
}
```

- Ta có thể dễ dàng nhận thấy thông qua file rp đó là thông tin nhạy cảm bị lộ chính là một API key

Task 7:

- Ngoài các bản ghi kể trên, hãy liệt kê các bản ghi khác của DNS.
- Sử dụng lệnh **host** để tìm kiếm các bản ghi TXT, MX cho tên miền uit.edu.vn

Trả lời:

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

Các bản ghi khác của DNS:

- AAAA (IPv6 Address Record): Bản ghi này tương tự như bản ghi A, nhưng thay vì trả về một địa chỉ IPv4, nó trả về địa chỉ IPv6 128-bit. Dùng để phân giải tên miền thành địa chỉ IPv6.
- SRV (Service Locator Record): Bản ghi SRV được sử dụng để chỉ định các dịch vụ cụ thể trên các máy chủ. Nó thường được sử dụng trong các ứng dụng như SIP (Session Initiation Protocol) hoặc XMPP (Extensible Messaging and Presence Protocol). Cấu trúc của SRV giúp định vị máy chủ cung cấp dịch vụ (ví dụ như VoIP, Chat, hay DNS).
- SOA (Start of Authority Record): Bản ghi SOA chỉ ra máy chủ DNS chính cho một khu vực DNS (zone) và các thông tin liên quan như số hiệu bản ghi, thời gian hết hạn của bản ghi, và các thông tin khác về khu vực DNS. Thông thường bản ghi SOA là bản ghi đầu tiên trong một khu vực DNS.
- NAPTR (Naming Authority Pointer): Bản ghi NAPTR được sử dụng trong các hệ thống phân giải tên gọi phức tạp như ENUM (E.164 Number Mapping) để ánh xạ số điện thoại sang các dịch vụ Internet.
- CAA (Certification Authority Authorization): Bản ghi CAA cho phép chủ sở hữu tên miền xác định các tổ chức chứng thực (CA) có quyền cấp chứng chỉ SSL/TLS cho tên miền của họ. Nó giúp ngăn ngừa việc cấp chứng chỉ SSL trái phép.
- DNAME (Delegation Name Record): Bản ghi DNAME cho phép tái cấu trúc các tên miền dưới một tên miền phụ. Nó có thể thay thế một miền bằng một miền khác và chuyển tiếp các yêu cầu DNS.
- MX (Mail Exchange): Cũng là một bản ghi quan trọng trong việc xử lý email, nhưng nhiều tên miền có thể có bản ghi MX cho các dịch vụ email khác nhau, giúp cân bằng tải hoặc cấu hình dự phòng.
- HINFO (Host Information Record): Bản ghi HINFO được sử dụng để cung cấp thông tin về hệ thống phần cứng và phần mềm của máy chủ. Tuy nhiên, bản ghi này ít được sử dụng trong các ứng dụng thực tế ngày nay.
- TXT (Text Record): Bản ghi TXT có thể chứa bất kỳ văn bản nào. Đây là bản ghi hữu ích trong việc triển khai các chính sách bảo mật, chẳng hạn như SPF (Sender Policy Framework) để xác minh nguồn gốc email hoặc DKIM (DomainKeys Identified Mail).

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

Các bản ghi TXT, MX cho tên miền uit.edu.vn:

```
(dducktai㉿kali)-[~]
$ host -t txt uit.edu.vn
uit.edu.vn descriptive text "sqm6y27vn74pm290pl0fq4hcr08gst5r"
uit.edu.vn descriptive text "v=spf1 include:_spf.google.com ~all"
uit.edu.vn descriptive text "google-site-verification=z9wIF5gp5-YbdAQsttR2KmyHCPy3FN6QkOGOBUWIrwc"
uit.edu.vn descriptive text "k6t321pqvf9jryb0z4n5scftqph6t781"
uit.edu.vn descriptive text "MS=E431E3CA3EFF5A6431E2378C924984A8A0334ABC"
uit.edu.vn descriptive text "google-site-verification=wjArKGa37oHK083Xqt2C91tPny8NLttGS0aU5pJjKiY"
uit.edu.vn descriptive text "_ukan9wll3iica6lscp6fwumq5v6dopw"
uit.edu.vn descriptive text "svp60rjlwr6s19rn9t013cfwm3xmqx7h"

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

Task 8: 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?

Trả lời:

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

(dducktai㉿kali)-[~]
$ 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

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

Nhận xét: Kết quả cho thấy rằng mặc dù các hostname không tồn tại, vẫn có địa chỉ IP được trả về cho tất cả các tên miền này. Có thể do một trong số các nguyên nhân sau:

- Hệ thống DNS đã lưu trữ thông tin từ các truy vấn trước đó. Khi một hostname đã từng tồn tại trong hệ thống DNS, các máy chủ DNS có thể lưu trữ địa chỉ IP của hostname đó trong một thời gian nhất định (TTL). Nếu TTL chưa hết, thông tin sẽ được trả về mặc dù hostname đó có thể không còn tồn tại.
- Hệ thống DNS sử dụng bản ghi wildcard (bản ghi DNS đại diện cho tất cả các tên miền không được khai báo cụ thể). Ví dụ, nếu *.uit.edu.vn được cấu hình trên máy chủ DNS của uit.edu.vn, bất kỳ tên miền nào không tồn tại cũng sẽ trả về một địa chỉ IP chung, ví dụ như 45.122.249.78 hoặc 118.69.123.140. Điều này có thể giải thích tại sao các tên miền không tồn tại vẫn trả về kết quả.
- Trong một số trường hợp, DNS server có thể chuyển hướng (forward) các yêu cầu cho các tên miền không tồn tại tới một địa chỉ IP mặc định. Điều này có thể được thực hiện

để giảm tải cho các DNS server hoặc như một biện pháp an ninh để ngăn chặn việc lây các lỗi DNS.

Task 9: Sử dụng wordlist thông dụng khác (rockyou, seclists) để tìm kiếm các hostname hợp lệ khác của megacorpone.com

Trả lời:

- Kết quả khi brute force toàn bộ subdomain trong rockyou:

```
(dducktai㉿kali)-[~]
$ dnsrecon -d megacorpone.com -t brt -D /usr/share/wordlists/rockyou.txt

[*] Using the dictionary file: /usr/share/dnsrecon/dnsrecon/data/namelist.txt
(provided by tool)
[*] brt: Performing host and subdomain brute force against megacorpone.com...
[+] A admin.megacorpone.com 167.114.21.64
[+] A beta.megacorpone.com 167.114.21.65
[+] A fs1.megacorpone.com 167.114.21.66
[+] A intranet.megacorpone.com 167.114.21.67
[+] A mail.megacorpone.com 167.114.21.68
[+] A mail2.megacorpone.com 167.114.21.69
[+] A ns3.megacorpone.com 66.70.207.180
[+] A ns1.megacorpone.com 51.79.37.18
[+] A ns2.megacorpone.com 51.222.39.63
[+] A router.megacorpone.com 167.114.21.70
[+] A siem.megacorpone.com 167.114.21.71
[+] A snmp.megacorpone.com 167.114.21.72
[+] A support.megacorpone.com 167.114.21.74
[+] A syslog.megacorpone.com 167.114.21.73
[+] A test.megacorpone.com 167.114.21.75
[+] A vpn.megacorpone.com 167.114.21.76
[+] A vpn2.megacorpone.com 167.114.21.77
[+] A www.megacorpone.com 149.56.244.87
[+] A www2.megacorpone.com 149.56.244.87
[+] 19 Records Found
```

- Kết quả khi brute force toàn bộ subdomain trong seclist:

```
(dducktai㉿kali)-[~]
$ dnsrecon -d megacorpone.com -t brt -D /home/dducktai/SecLists/Discovery/DNS/subdomains-top1million-110000.txt

[*] Using the dictionary file: /usr/share/dnsrecon/dnsrecon/data/namelist.txt
(provided by tool)
[*] brt: Performing host and subdomain brute force against megacorpone.com...
[+] A admin.megacorpone.com 167.114.21.64
[+] A beta.megacorpone.com 167.114.21.65
[+] A fs1.megacorpone.com 167.114.21.66
[+] A intranet.megacorpone.com 167.114.21.67
[+] A mail2.megacorpone.com 167.114.21.69
[+] A mail.megacorpone.com 167.114.21.68
[+] A ns2.megacorpone.com 51.222.39.63
[+] A ns1.megacorpone.com 51.79.37.18
[+] A ns3.megacorpone.com 66.70.207.180
[+] A router.megacorpone.com 167.114.21.70
[+] A siem.megacorpone.com 167.114.21.71
[+] A snmp.megacorpone.com 167.114.21.72
[+] A support.megacorpone.com 167.114.21.74
[+] A syslog.megacorpone.com 167.114.21.73
[+] A test.megacorpone.com 167.114.21.75
[+] A vpn.megacorpone.com 167.114.21.76
[+] A vpn2.megacorpone.com 167.114.21.77
[+] A www.megacorpone.com 149.56.244.87
[+] A www2.megacorpone.com 149.56.244.87
[+] 19 Records Found
```

Task 10: Viết một chương trình Bash script để liệt kê danh sách các nameserver của các đơn vị thành viên thuộc Đại học Quốc Gia TP.HCM (hcmus.edu.vn, hcmussh.edu.vn, uit.edu.vn, hcmut.edu.vn, hcmiu.edu.vn, uel.edu.vn, hcmler.edu.vn, vnuhcm.edu.vn) và thực hiện zone transfer ứng với các nameserver đã tìm được.

Trả lời:

- File main.sh:

```
#!/bin/bash

# Định nghĩa danh sách các domain
domains=("hcmus.edu.vn" "hcmussh.edu.vn" "uit.edu.vn" "hcmut.edu.vn" "hcmiu.edu.vn"
"uel.edu.vn" "hcmler.edu.vn" "vnuhcm.edu.vn")

# Tạo file kết quả hoặc mở file để ghi kết quả
output_file="zone_transfer_results.txt"
> $output_file # Làm trống file nếu file đã tồn tại

# Lặp qua từng domain
for domain in ${domains[@]}; do
    echo "Performing zone transfer for domain: $domain" | tee -a $output_file

    # Lấy danh sách các nameserver cho domain
    for nameServer in $(host -t ns $domain 2>/dev/null | cut -d " " -f 4); do
        echo "Using nameserver: $nameServer" | tee -a $output_file

        # Thực hiện zone transfer và lưu kết quả vào file
        echo "Performing zone transfer..." | tee -a $output_file
        host -l $domain $nameServer 2>/dev/null | tee -a $output_file

        echo "-----### End of zone transfer for $domain ###-----" | tee -a $output_file
        echo | tee -a $output_file
    done

    echo "-----### End of processing for $domain ###-----" | tee -a $output_file
    echo | tee -a $output_file
done
```

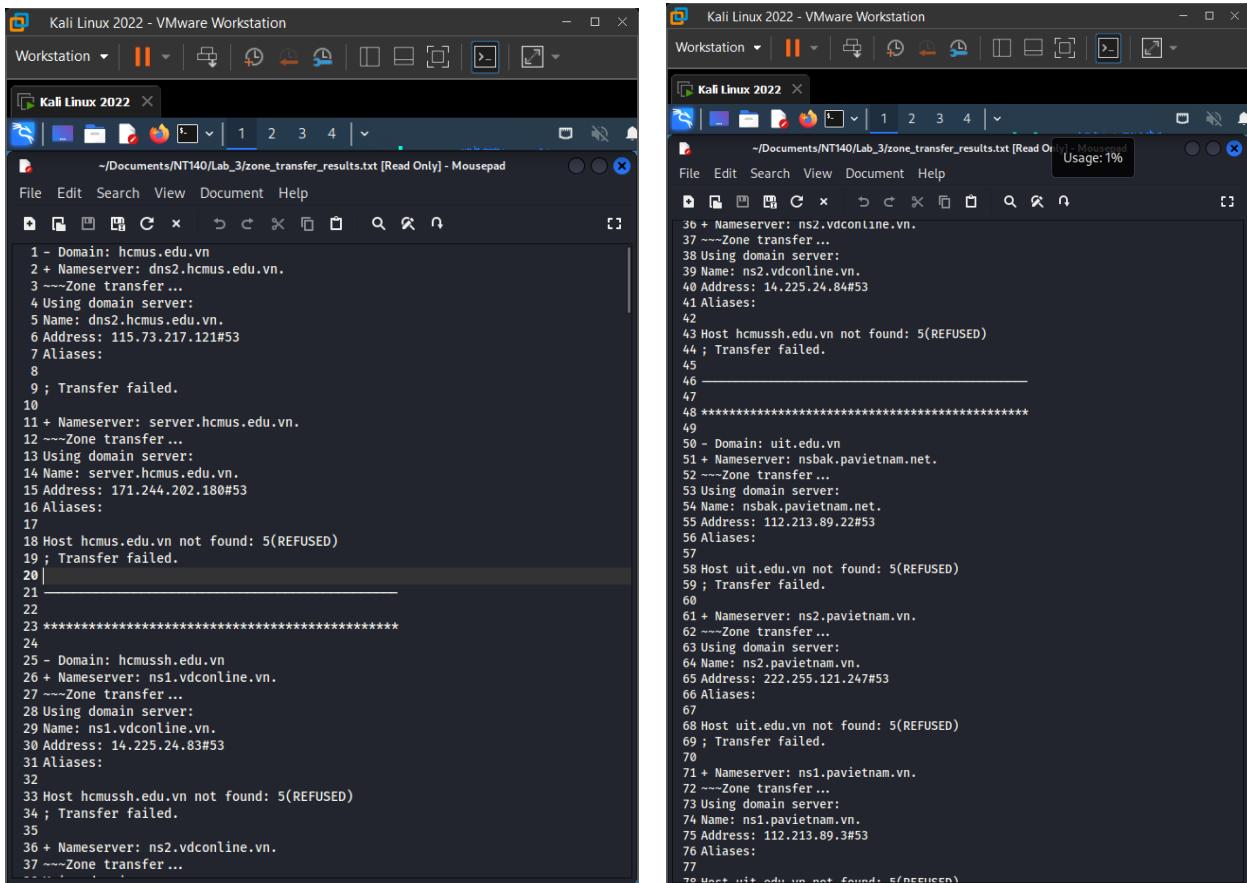
- Kết quả:

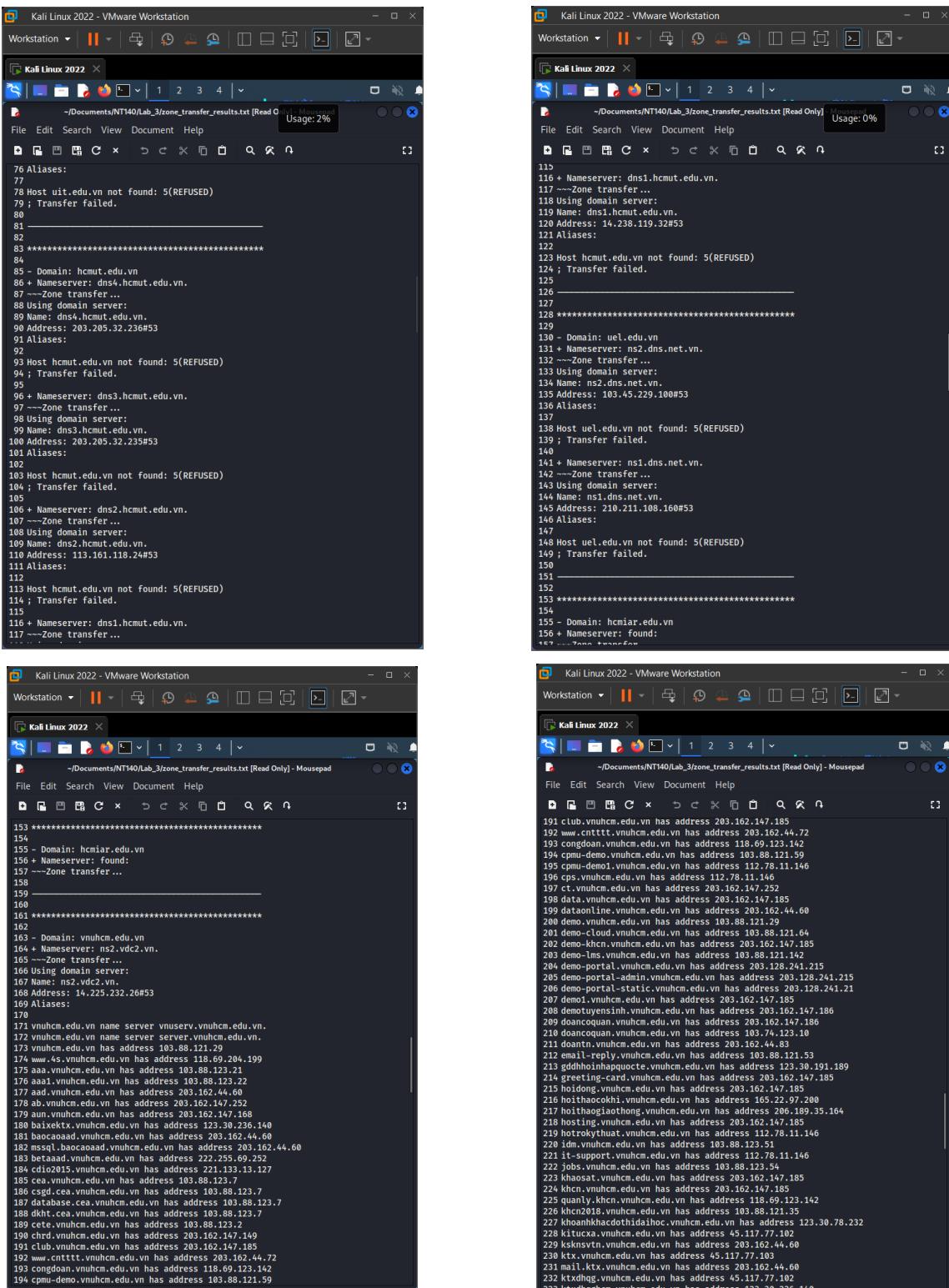
```
[root@kali]~[~/Documents/NT140/Lab_3]
# ./main.sh
Performing zone transfer for domain: hcmus.edu.vn
Using nameserver: server.hcmus.edu.vn.
Performing zone transfer ...
Using domain server:
Name: server.hcmus.edu.vn.
Address: 171.244.202.180#53
Aliases:
Host hcmus.edu.vn not found: 5(REFUSED)
; Transfer failed.
=====
### End of zone transfer for hcmus.edu.vn ###

Places
Using nameserver: dns2.hcmus.edu.vn.
Performing zone transfer ...
Using domain server:
Name: dns2.hcmus.edu.vn.
Address: 115.73.217.121#53
Aliases:
; Transfer failed.
=====
### End of zone transfer for hcmus.edu.vn ###

zone-transfer-result
=====
### End of processing for hcmus.edu.vn ###

Performing zone transfer for domain: hcmussh.edu.vn
Using nameserver: ns1.vdconline.vn.
Performing zone transfer ...
Using domain server:
```





Task 11: Thực hiện bắt Wireshark để mô tả cách gói tin được gửi và nhận khi thực hiện SYN Scan, TCP Connect Scan, UDP Scan sử dụng Nmap. So sánh với sử dụng phương thức các phương thức này với nhau (số lượng gói tin được gửi, số lượng gói tin được nhận, thời gian quét, kết quả hiển thị...)

Trả lời:

* Thực hiện SynScan:

```
(kali㉿kali)-[~]
$ sudo nmap -sS 42.96.18.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 11:40 +07

(kali㉿kali)-[~]
$ sudo nmap -sS 42.96.18.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 11:40 +07
Nmap scan report for 42.96.18.79
Host is up (0.016s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3306/tcp  open  mysql
8000/tcp  open  http-alt
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 5.21 seconds
```

- Từ kết quả của nmap, ta thấy port 80 đang mở, quan sát trong wireshark ta thấy:

tcp.port == 80						
No.	Time	Source	Destination	Protocol	Length	Info
10	0.915825548	192.168.31.130	42.96.18.79	TCP	54	37907 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
12	0.916576142	42.96.18.79	192.168.31.130	TCP	60	80 → 37907 [RST] Seq=1 Win=32767 Len=0
62	2.783456608	192.168.31.130	42.96.18.79	TCP	58	38163 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
79	2.807895187	42.96.18.79	192.168.31.130	TCP	60	80 → 38163 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
83	2.807981976	192.168.31.130	42.96.18.79	TCP	54	38163 → 80 [RST] Seq=1 Win=0 Len=0
1691	5.322024183	192.168.31.130	42.96.18.79	TCP	54	38168 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
1696	5.322194020	42.96.18.79	192.168.31.130	TCP	60	80 → 38168 [RST] Seq=1 Win=32767 Len=0

- + Gói 62 Máy ta gửi 1 gói tin đến SYN đến đích là 42.96.18.79
- + Gói 79 địa chỉ 42.96.18.79 gửi lại gói SYN và ACK tới máy ta để bắt tay 3 bước
- + Gói 83 Máy ta gửi 42.96.18.79 gói RST để đóng kết nối

- Ngoài ra ta cũng thấy được port 125 đang đóng nên ta thực hiện kiểm tra wireshark thấy được:

No.	Time	Source	Destination	Protocol	Length	Info
1948	5.593943738	192.168.31.130	42.96.18.79	TCP	58	38163 → 125 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2044	5.700845232	192.168.31.130	42.96.18.79	TCP	58	38165 → 125 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2259	8.345841183	42.96.18.79	192.168.31.130	TCP	60	125 → 38163 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0

+ Gói 1948 và 2044 Máy ta gửi đến 42.96.18.79 một SYN

+ Máy 42.96.18.79 trả cho máy ta gói RST, ACK

⇒ Port 125 đang đóng

* Thực hiện TCP Connect Scan

```
(kali㉿kali)-[~]
$ sudo nmap -sT 42.96.18.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 11:47 +07
Nmap scan report for 42.96.18.79
Host is up (0.0084s latency).

Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3306/tcp  open  mysql
8000/tcp  open  http-alt
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 7.07 seconds
```

- Tiếp tục kiểm tra port 80 tương tự như Syn ta có kết quả như sau:

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000161137	192.168.31.130	42.96.18.79	TCP	54	47645 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
5	0.000728734	42.96.18.79	192.168.31.130	TCP	60	80 → 47645 [RST] Seq=1 Win=32767 Len=0
68	1.897214687	192.168.31.130	42.96.18.79	TCP	74	46846 → 89 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=4201234532 TSecr=0 WS=128
79	1.996603863	42.96.18.79	192.168.31.130	TCP	60	80 → 46846 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
80	1.996618261	192.168.31.130	42.96.18.79	TCP	54	46846 → 80 [ACK] Seq=1 Ack=1 Win=32120 Len=0
88	1.997376938	192.168.31.130	42.96.18.79	TCP	54	46846 → 80 [RST, ACK] Seq=1 Ack=1 Win=32120 Len=0

+ Gói 68 Máy ta gửi 1 gói tin SYN đến đích là 42.96.18.79

+ Gói 79 địa chỉ 42.96.18.79 gửi lại gói SYN và ACK tới máy ta để bắt tay 3 bước

+ gói 80 và 88 Máy ta gửi 42.96.18.79 gói ACK,RST để đóng kết nối

- Tương tự cho port 125:

No.	Time	Source	Destination	Protocol	Length	Info
1501	4.461317279	192.168.31.130	42.96.18.79	TCP	74	45532 → 125 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TStamp=4201237096 TSect=0 WS=128
1588	4.564810120	192.168.31.130	42.96.18.79	TCP	74	45548 → 125 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TStamp=4201237200 TSect=0 WS=128
2705	16.444118532	42.96.18.79	192.168.31.130	TCP	60	125 → 45548 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0

+ Gói 1948 và 2044 Máy ta gửi đến 42.96.18.79 một SYN

+ Máy 42.96.18.79 trả cho máy ta gói RST, ACK

⇒ Port 125 đóng

* UDP scan

```
(kali㉿kali)-[~]
$ sudo nmap -sU 42.96.18.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 11:55 +07
Nmap scan report for 42.96.18.79
Host is up (0.0013s latency).
All 1000 scanned ports on 42.96.18.79 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 1599.69 seconds
```

- Từ kết quả của nmap, ta thấy không có port nào mở cả, ta thực hiện kiểm thử trong Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000173061	192.168.31.130	42.96.18.79	TCP	54	45990 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
5	0.0001484360	42.96.18.79	192.168.31.130	TCP	60	80 → 45990 [RST] Seq=1 Win=32767 Len=0
31	1.329643182	192.168.31.130	42.96.18.79	TCP	54	46251 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
32	1.329877397	42.96.18.79	192.168.31.130	TCP	60	80 → 46251 [RST] Seq=1 Win=32767 Len=0
56	2.640643821	192.168.31.130	42.96.18.79	TCP	54	46253 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
57	2.641525345	42.96.18.79	192.168.31.130	TCP	60	80 → 46253 [RST] Seq=1 Win=32767 Len=0
70	3.954671975	192.168.31.130	42.96.18.79	TCP	54	46255 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
71	3.954955179	42.96.18.79	192.168.31.130	TCP	60	80 → 46255 [RST] Seq=1 Win=32767 Len=0
88	5.266961758	192.168.31.130	42.96.18.79	TCP	54	46257 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
89	5.267215044	42.96.18.79	192.168.31.130	TCP	60	80 → 46257 [RST] Seq=1 Win=32767 Len=0
102	6.575150859	192.168.31.130	42.96.18.79	TCP	54	46259 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
103	6.575558736	42.96.18.79	192.168.31.130	TCP	60	80 → 46259 [RST] Seq=1 Win=32767 Len=0
116	7.885697013	192.168.31.130	42.96.18.79	TCP	54	46261 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
117	7.886102287	42.96.18.79	192.168.31.130	TCP	60	80 → 46261 [RST] Seq=1 Win=32767 Len=0
130	9.195749575	192.168.31.130	42.96.18.79	TCP	54	46263 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
131	9.196722560	42.96.18.79	192.168.31.130	TCP	60	80 → 46263 [RST] Seq=1 Win=32767 Len=0
144	10.503500270	192.168.31.130	42.96.18.79	TCP	54	46265 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
145	10.503798772	42.96.18.79	192.168.31.130	TCP	60	80 → 46265 [RST] Seq=1 Win=32767 Len=0

+ Liên tục là những lần gửi ACK từ máy ta và nhận về gói tin RST từ địa chỉ 42.96.18.79

⇒ Không có port 80 (kết quả tương tự cho các port khác) đang mở

Task 12:

- Thực hiện kiểm tra các host đang hoạt động trong mạng bằng các ngôn ngữ lập trình khác (Bashscript, Python, C/C++, Perl, ...).
- Sử dụng Wireshark để phân tích gói tin khi sử dụng Nmap với tùy chọn -sn

Trả lời:

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

- Thực hiện bằng đoạn code task4.sh

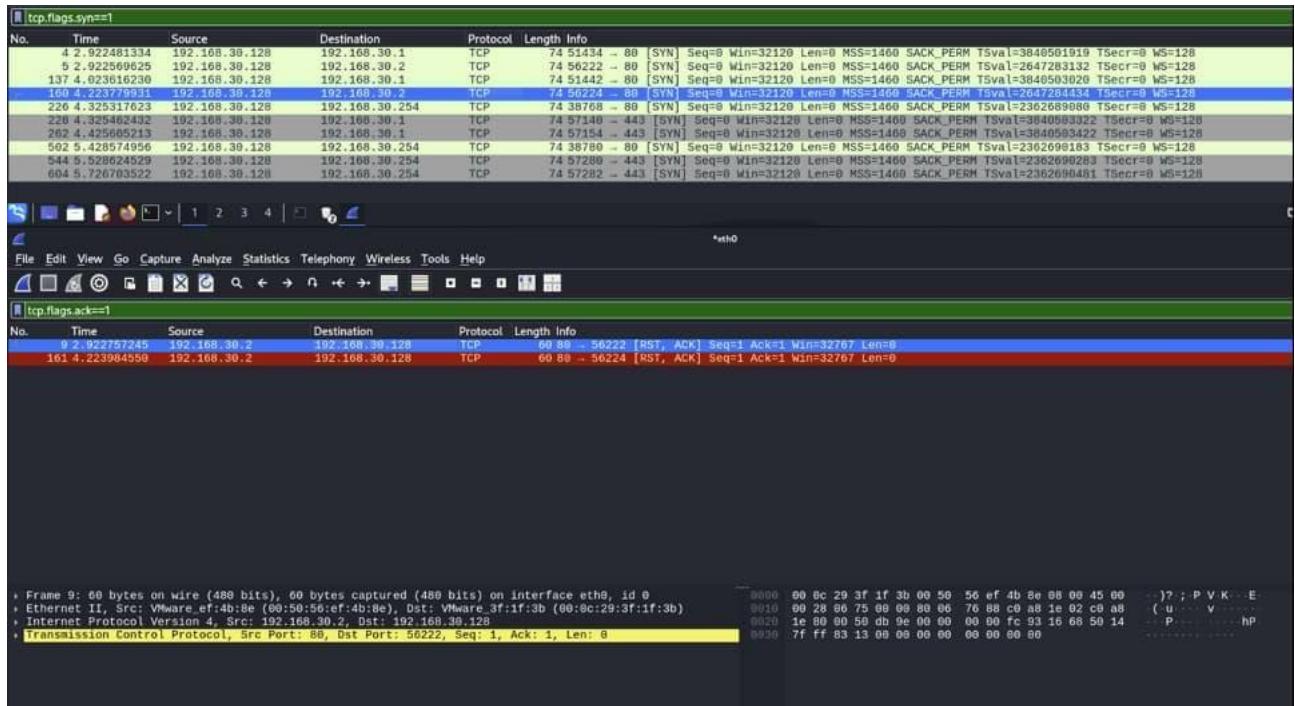
```
GNU nano 4.8                               task4.sh
#!/bin/bash
sudo nmap -v -sn 192.168.23.129-254 -oG ping-sweep.txt
grep Up ping-sweep.txt | cut -d " " -f 2
```

```
hohuy@ubuntu:~$ ./task4.sh
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-16 02:23 PST
Initiating Ping Scan at 02:23
Scanning 126 hosts [4 ports/host]
Ping Scan Timing: About 31.75% done; ETC: 02:24 (0:01:07 remaining)
Completed Ping Scan at 02:23, 37.19s elapsed (126 total hosts)
Initiating Parallel DNS resolution of 126 hosts. at 02:23
Completed Parallel DNS resolution of 126 hosts. at 02:23, 0.40s elapsed
Nmap scan report for 192.168.23.129
Host is up (0.00049s latency).
```

- Kết quả:

```
Nmap scan report for 192.168.23.254
Host is up (0.00049s latency).
Read data files from: /usr/bin/../share/nmap
Nmap done: 126 IP addresses (126 hosts up) scanned in 37.63 seconds
    Raw packets sent: 830 (31.056KB) | Rcvd: 126 (5.040KB)
192.168.23.129
192.168.23.130
192.168.23.131
```

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



Task 13:

- a. *Liệt kê các banner, dịch vụ đang chạy trên máy Metasploitable 2 (chỉ liệt kê các dịch vụ TCP).*
- b. *Sử dụng thêm 2 NSE script (tự chọn) để quét máy mục tiêu (Metasploitable 2)*

Trả lời:

- a. *Liệt kê các banner, dịch vụ đang chạy trên máy Metasploitable 2 (chỉ liệt kê các dịch vụ TCP).*

- Địa chỉ ip của máy Metasploitable 2:

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:76:57:68
          inet addr:192.168.31.129 Bcast:192.168.31.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe76:5768/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                  RX packets:4 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:64 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:989 (989.0 B) TX bytes:5596 (5.4 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:121 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:121 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:0
                  RX bytes:27197 (26.5 KB) TX bytes:27197 (26.5 KB)

msfadmin@metasploitable:~$
```

- Thực hiện lệnh: nmap -sV -sT -A 192.168.31.129

+ -sV: Phát hiện phiên bản của dịch vụ đang chạy trên các cổng mở

+ -sT: Thực hiện quét TCP kết nối đầy đủ (Connect Scan). Đây là cách quét TCP mặc định khi bạn không có quyền root.

+ -A: Kích hoạt các tùy chọn quét nâng cao:

- Phát hiện hệ điều hành (OS Detection)
- Phát hiện phiên bản dịch vụ
- Chạy script Nmap (NSE) để tìm kiếm thêm thông tin chi tiết
- Theo dõi dấu thời gian hop (traceroute)

- Kết quả:

```
(kali㉿kali)-[~]
└─$ nmap -sV -sT -A 192.168.31.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 16:18 +07
Stats: 0:01:44 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.23% done; ETC: 16:19 (0:00:02 remaining)
Nmap scan report for 192.168.31.129
Host is up (0.0032s 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 192.168.31.130
|   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:cfe:1:c0:5f:6a:74:d6:40:fa:c4:d5:6c:cd (DSA)
|   1024 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
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind     2 (RPC #100000)
|_rpcinfo: ERROR: Script execution failed (use -d to debug)
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?
514/tcp   open  shell        Netkit rshd
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


```

```
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql      MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 13
|   Capabilities flags: 43564
|   Some Capabilities: SwitchToSSLAfterHandshake, SupportsTransactions, Support41Auth, Speaks41ProtocolNew, SupportsCompression, ConnectWithDatabase, LongColumnFlag
|   Status: Autocommit
|_ Salt: X.z@{xG<3.*(+=2"S\W
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: 2024-11-16T09:20:26+00:00; +6s from scanner time.
5900/tcp open  vnc        VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_  VNC Authentication (2)
6000/tcp open  X11        (access denied)
6667/tcp open  irc        UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:14:38
|   source ident: nmap
|   source host: 221E595D.EDAFDF4B.FFFA6D49.IP
|_ error: Closing Link: mbstxxxkl[192.168.31.130] (Quit: mbstxxxkl)
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-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
MAC Address: 00:0C:29:76:57:68 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```

OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|   System time: 2024-11-16T04:19:04-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
| smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h40m05s, deviation: 2h53m12s, median: 5s
|_nbstat: NetBIOS name: METASPOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT      ADDRESS
1  3.18 ms  192.168.31.129

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 142.35 seconds

```

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

- Di chuyển vào thư mục /usr/share/nmap/scripts để xem các lệnh NSE khác

```

(kali㉿kali)-[~]
$ cd /usr/share/nmap/scripts
(kali㉿kali)-[/usr/share/nmap/scripts]
$ ls
acardd-info.nse          finger.nse           http-svn-enum.nse        ms-sql-tables.nse      smb-print-text.nse
address-info.nse          fingerprint-strings.nse  http-svn-info.nse       ms-sql-xp-cmdshell.nse  smb-protocols.nse
afp-brute.nse             firewall.nse         http-title.nse         mtrace.nse            smb-psexec.nse
afp-ls.nse                firewall-bypass.nse    http-tplink-dir-traversals.nse  murmur-version.nse   smb-security-mode.nse
afp-path-vuln.nse          flume-master-info.nse  http-trace.nse         mysql-audit.nse      smb-server-stats.nse
afp-serverinfo.nse         fox-info.nse        http-traceroute.nse   mysql-brute.nse     smb-system-info.nse
afp-showmount.nse          freelancer.info.nse  http-trame-info.nse   mysql-databases.nse  smb-vuln-conficker.nse
ajp-auth.nse               ftp-anon.nse        http-unsafe-output-escaping.nse  mysql-dump-hashes.nse  smb-vuln-cve2009-3103.nse
ajp-brute.nse              ftp-bounce.nse       http-useragent-tester.nse  mysql-empty-password.nse  smb-vuln-cve-2017-7494.nse
ajp-headers.nse            ftp-brute.nse       http-userdir-enum.nse   mysql-enum.nse      smb-vuln-ms06-025.nse
ajp-methods.nse            ftp-libopie.nse     http-vhosts.nse        mysql-info.nse      smb-vuln-ms07-029.nse
ajp-request.nse            ftp-proftpd-backdoor.nse  http-virustotal.nse   mysql-query.nse     smb-vuln-ms08-067.nse
allseeingeye-info.nse     ftp-vsftpd-backdoor.nse  http-vlcstreamer-ls.nse  mysql-users.nse     smb-vuln-ms10-054.nse
amqp-info.nse              ftp-vuln-cve2006-4221.nse  http-vmware-path-vuln.nse  mysql-variables.nse  smb-vuln-ms10-061.nse
asn-query.nse              ftp-vuln-cve2009-392.nse   http-vuln-cve2012-2122.nse  myssql-vuln-nse     smb-vuln-ms17-010.nse
auth-owners.nse            ganglia-info.nse    http-vuln-cve2009-396.nse  nat-mpm-info.nse   smb-vuln-regsvc-dos.nse
auth-spoof.nse             giop-info.nse       http-vuln-cve2010-0738.nse  nat-mpm-mapproap.nse  smb-vuln-webexec.nse
backorifice-brute.nse     gkrellm-info.nse   http-vuln-cve2010-2861.nse  nbd-info.nse      smb-webexec-exploit.nse
backorifice-info.nse       gopher-ls.nse       http-vuln-cve2011-3192.nse  nbns-interfaces.nse  sntp-brute.nse
bacnet-info.nse            gpsd-info.nse      http-vuln-cve2011-3368.nse  nbstat.nse       sntp-commands.nse
banner.nse                hadoop-datanode-info.nse  http-vuln-cve2012-1823.nse  ncp-nms.nse      sntp-enum-users.nse
bitcoin-getaddr.nse        hadoop-jobtracker-info.nse  http-vuln-cve2013-0156.nse  ncp-serverinfo.nse  sntp-htnl-infos.nse
bitcoin-info.nse           hadoop-namenode-info.nse  http-vuln-cve2013-6786.nse  ndmp-fs-info.nse   sntp-open-relay.nse
bitcoinrpc-info.nse        hadoop-secondary-namenode-info.nse  http-vuln-cve2013-7091.nse  ndmp-version.nse  smtp-strangeport.nse
bittorrent-discovery.nse   hadoop-tasktracker-info.nse  http-vuln-cve2014-2126.nse  nessus-brute.nse  smtp-vuln-cve2010-4344.nse
bjnp-discover.nse          hbase-master-info.nse  http-vuln-cve2014-2127.nse  nessus-xmllrcp-brute.nse  smtp-vuln-cve2011-1720.nse
broadcast-ataeo-discover.nse  hbase-region-info.nse  http-vuln-cve2014-2128.nse  netbus-auth-bypass.nse  smtp-vuln-cve2011-1764.nse
broadcast-avahi-dos.nse    hdtemp-info.nse     http-vuln-cve2014-2129.nse  netbus-brute.nse  sniffer-detect.nse
broadcast-bjnp-discover.nse  hbaseinfo.nse      http-vuln-cve2014-3704.nse  netbus-info.nse   snmp-brute.nse
broadcast-db2-discover.nse  hostmap-bfk.nse    http-vuln-cve2014-4277.nse  nexpose-brute.nse  snmp-h3c-logins.nse
broadcast-dhcp-discover.nse  hostmap-crthsh.nse  http-vuln-cve2015-1427.nse  nfs-ls.nse       snmp-info.nse
broadcast-dns-service-discovery.nse  hostmap-robtex.nse  http-vuln-cve2015-1635.nse  nfs-showmount.nse  snmp-interfaces.nse
broadcast-dropbox-listener.nse  http-adobe-coldfusion-apsla1301.nse  http-vuln-cve2017-100100.nse  nfs-statfs.nse   snmp-los-config.nse
broadcast-eigrp-discovery.nse  http-affiliate-id.nse  http-vuln-cve2017-5638.nse  nje-node-brute.nse  snmp-netstat.nse
broadcast-igmp-discovery.nse  http-apache-negotiation.nse  http-vuln-cve2017-5689.nse  nje-pass-brute.nse  snmp-processes.nse
broadcast-jenkins-discover.nse  http-apache-server-status.nse  http-vuln-cve2017-9917.nse  nrpe-nse       snmp-sysdescr.nse
broadcast-listener.nse      http-aspnets-debug.nse  http-vuln-misfortune-cookies.nse  nrpe-enum.nse   snmp-win32-services.nse
broadcast-ms-sql-discover.nse  http-auth-finder.nse  http-vuln-wm1000-creds.nse  nrpe-fingerprint.nse  snmp-win32-shares.nse
broadcast-nethios-master-browser.nse  http-auth-nse   http-waf-detect.nse      nrpe-info.nse   snmp-win32-software.nse
                                http-avaya-ipoffice-users.nse  http-waf-fingerprint.nse  nrpe-monlist.nse  snmp-win32-users.nse
                                http-awstatsinfoexec.nse  http-webday-scan.nse

```

- Lệnh 1: nmap -sV --script=banner 192.168.23.129

+ -sV: Phát hiện phiên bản dịch vụ đang chạy

+ --script=banner: Sử dụng script NSE banner để thu thập thông tin tiêu đề (banner) từ các cổng mở

+ Script này hoạt động tốt với các dịch vụ như HTTP, FTP, SSH, SMTP, và nhiều dịch vụ khác

⇒ Banner thường giúp xác định thêm thông tin từ dịch vụ, như phiên bản chính xác

```
(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap -sV --script=banner 192.168.31.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 16:24 +07
Nmap scan report for 192.168.31.129
Host is up (0.0071s latency).

Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_banner: 220 (vsFTPD 2.3.4)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
23/tcp    open  telnet       Linux telnetd
|_banner: \xFF\xFD\x18\xFF\xFD\xFF\xFD#\xFF\xFD'
25/tcp    open  smtp         Postfix smtpd
|_banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
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     48448/udp  mountd
|   100005  1,2,3     50034/tcp   mountd
|   100021  1,3,4     52236/tcp   nlockmgr
|   100021  1,3,4     53542/udp   nlockmgr
|   100024  1          44418/tcp   status
|   100024  1          60099/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
|_banner: \x01Where are you?
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
|_banner: \x01getnameinfo: Temporary failure in name resolution
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
|_banner: root@metasploitable:/#
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
|_banner: 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.31.129]
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
```

```
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
|_banner: \x01Where are you?
513/tcp open  login?
514/tcp open  shell      Netkit rshd
|_banner: \x01getnameinfo: Temporary failure in name resolution
1099/tcp open  java-rmi   GNU Classpath grmiregistry
1524/tcp open  bindshell  Metasploitable root shell
|_banner: root@metasploitable:/
2049/tcp open  nfs       2-4 (RPC #100003)
2121/tcp open  ftp       ProFTPD 1.3.1
|_banner: 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.31.129]
3306/tcp open  mysql     MySQL 5.0.51a-3ubuntu5
|_banner: >\x00\x00\x00\x0A5.0.51a-3ubuntu5\x00\x14\x00\x00\x00\x01.20x/~N\x
|_00,\xA0\x08\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00...
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc       VNC (protocol 3.3)
|_banner: RFB 003.003
6000/tcp open  X11       (access denied)
6667/tcp open  irc       UnrealIRCd
|_banner: :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostna
|_me...
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:29:76:57:68 (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 66.19 seconds
```

- Lệnh 2: nmap --script=smb-enum-shares,smb-enum-users -p 445 192.168.23.129
 - + --script=smb-enum-users: Liệt kê thông tin người dùng SMB nếu có thể
 - + --script=smb-enum-shares: Liệt kê các chia sẻ SMB trên mục tiêu
 - + -p 445: Chỉ quét cổng SMB (445), nơi dịch vụ chia sẻ thường hoạt động
 - ⇒ Lệnh này hữu ích trong môi trường nội bộ để kiểm tra quyền truy cập chia sẻ mạng và các tài khoản người dùng SMB

```
(kali㉿kali)-[/usr/share/nmap/scripts]
$ nmap --script=smb-enum-shares,smb-enum-users -p 445 192.168.31.129

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 16:40 +07
Nmap scan report for 192.168.31.129
Host is up (0.0038s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 00:0C:29:76:57:68 (VMware)

Host script results:
| smb-enum-users:
|   METASPLOITABLE\backup (RID: 1068)
|     Full name: backup
|     Flags:      Account disabled, Normal user account
|   METASPLOITABLE\bin (RID: 1004)
|     Full name: bin
|     Flags:      Account disabled, Normal user account
|   METASPLOITABLE\bind (RID: 1210)
|     Flags:      Account disabled, Normal user account
|   METASPLOITABLE\daemon (RID: 1002)
|     Full name: daemon
|     Flags:      Account disabled, Normal user account
|   METASPLOITABLE\dhcp (RID: 1202)
|     Flags:      Account disabled, Normal user account
|   METASPLOITABLE\distccd (RID: 1222)
|     Flags:      Account disabled, Normal user account
|   METASPLOITABLE\ftp (RID: 1214)
|     Flags:      Account disabled, Normal user account
|   METASPLOITABLE\games (RID: 1010)
|     Full name: games
|     Flags:      Account disabled, Normal user account
|   METASPLOITABLE\gnats (RID: 1082)
|     Full name: Gnats Bug-Reporting System (admin)
|     Flags:      Account disabled, Normal user account
|   METASPLOITABLE\irc (RID: 1078)
|     Full name: ircd
|     Flags:      Account disabled, Normal user account
|   METASPLOITABLE\klog (RID: 1206)
|     Flags:      Account disabled, Normal user account
|   METASPLOITABLE\libuuid (RID: 1200)
|     Flags:      Account disabled, Normal user account
|   METASPLOITABLE\list (RID: 1076)
|     Full name: Mailing List Manager
|     Flags:      Account disabled, Normal user account
```

```
METASPLOITABLE\klog (RID: 1200)
Flags:      Account disabled, Normal user account
METASPLOITABLE\libuuid (RID: 1200)
Flags:      Account disabled, Normal user account
METASPLOITABLE\list (RID: 1076)
Full name:  Mailing List Manager
Flags:      Account disabled, Normal user account
METASPLOITABLE\lp (RID: 1014)
Full name:  lp
Flags:      Account disabled, Normal user account
METASPLOITABLE\mail (RID: 1016)
Full name:  mail
Flags:      Account disabled, Normal user account
METASPLOITABLE\man (RID: 1012)
Full name:  man
Flags:      Account disabled, Normal user account
METASPLOITABLE\msfadmin (RID: 3000)
Full name:  msfadmin,,
Flags:      Normal user account
METASPLOITABLE\mysql (RID: 1218)
Full name:  MySQL Server,,
Flags:      Account disabled, Normal user account
METASPLOITABLE\news (RID: 1018)
Full name:  news
Flags:      Account disabled, Normal user account
METASPLOITABLE\nobody (RID: 501)
Full name:  nobody
Flags:      Account disabled, Normal user account
METASPLOITABLE\postfix (RID: 1212)
Flags:      Account disabled, Normal user account
METASPLOITABLE\postgres (RID: 1216)
Full name:  PostgreSQL administrator,,
Flags:      Account disabled, Normal user account
METASPLOITABLE\proftpd (RID: 1226)
Flags:      Account disabled, Normal user account
METASPLOITABLE\proxy (RID: 1026)
Full name:  proxy
Flags:      Account disabled, Normal user account
METASPLOITABLE\root (RID: 1000)
Full name:  root
Flags:      Account disabled, Normal user account
METASPLOITABLE\service (RID: 3004)
Full name:  ,,
Flags:      Account disabled, Normal user account
METASPLOITABLE\sshd (RID: 1208)
Flags:      Account disabled, Normal user account
```

```
Flags:      Account disabled, Normal user account
METASPLOITABLE\www-data (RID: 1066)
  Full name: www-data
  Flags:      Account disabled, Normal user account
smb-enum-shares:
  account_used: <blank>
  \\192.168.31.129\ADMIN$:
    Type: STYPE_IPC
    Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
    Users: 1
    Max Users: <unlimited>
    Path: C:\tmp
    Anonymous access: <none>
  \\192.168.31.129\IPC$:
    Type: STYPE_IPC
    Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
    Users: 1
    Max Users: <unlimited>
    Path: C:\tmp
    Anonymous access: READ/WRITE
  \\192.168.31.129\opt:
    Type: STYPE_DISKTREE
    Comment:
    Users: 1
    Max Users: <unlimited>
    Path: C:\tmp
    Anonymous access: <none>
  \\192.168.31.129\print$:
    Type: STYPE_DISKTREE
    Comment: Printer Drivers
    Users: 1
    Max Users: <unlimited>
    Path: C:\var\lib\samba\printers
    Anonymous access: <none>
  \\192.168.31.129\tmp:
    Type: STYPE_DISKTREE
    Comment: oh noes!
    Users: 1
    Max Users: <unlimited>
    Path: C:\tmp
    Anonymous access: READ/WRITE

```

Nmap done: 1 IP address (1 host up) scanned in 13.61 seconds

Task 14:

- Thực hiện lại các bước trên để quét máy Metasploitable 2 không sử dụng tài khoản chứng thực.
- Bật Wireshark sau đó tiến hành quét và xác định các bước mà Nessus đã thực hiện để hoàn tất quá trình quét.
- Quét lại nhưng quét thêm port UDP.

Trả lời:

- a. Thực hiện lại các bước trên để quét máy Metasploitable 2 không sử dụng tài khoản chứng thực.**

- Hoàn tất quét:

Metasploitable2 - Basic

Configure Audit Trail Plugins are done compiling.

Hosts 1 Vulnerabilities 70 Remediations 3 History 1

Search History 1 History

Last Scanned Status Scan Details

Start Time ▾ Last Scanned Status Policy: Basic Network Scan
Current Today at 8:43 AM Today at 8:52 AM Completed Completed
Scanner: Local Scanner Severity Base: CVSS v3.0
Start: Today at 8:43 AM End: Today at 8:52 AM Elapsed: 9 minutes

Vulnerabilities

Critical: 0 High: 0 Medium: 0 Low: 0 Info: 12

Metasploitable2 - Basic / 192.168.31.4

Configure Audit Trail Launch Report Export

Vulnerabilities 12

Filter Search Vulnerabilities 12 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
Critical	10.0 *	7.4	0.6661	UnrealIRCd Backdoor Detection	Backdoors	1
Critical	10.0 *	5.1	0.1175	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	Gain a shell remotely	2
Critical	10.0 *	5.1	0.1175	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Gain a shell remotely	1
Critical	9.8	9.0	0.9737	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
High	8.6	5.2	0.0164	ISC BIND Service Downgrade / Reflected DoS	DNS	1
High	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	1
High	7.5 *	5.9	0.015	rsh Service Detection	Service detection	1
Medium	6.8	6.0	0.1395	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	DNS	1
Medium	5.9	4.4	0.9717	ISC BIND Denial of Service	DNS	1
Medium	5.3			SMB Signing not required	Misc.	1
Medium	4.0 *	7.3	0.0114	SMTP Service STARTTLS Plaintext Command Injection	SMTP problems	1
Low	3.4	5.1	0.9749	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	General	2

Host Details

IP: 192.168.31.4
MAC: 00:0C:29:10:D1:5C
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 8:43 AM
End: Today at 8:52 AM
Elapsed: 9 minutes
KB: Download

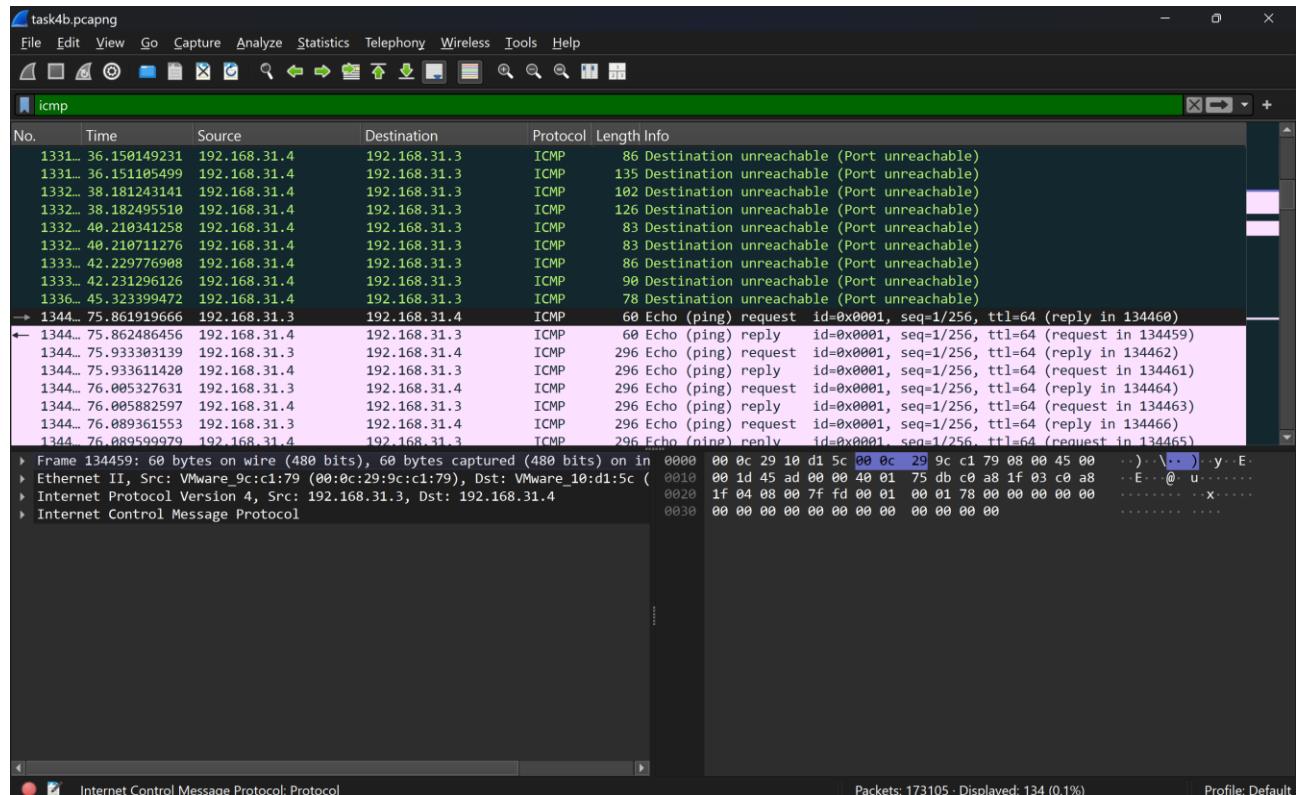
Vulnerabilities

Critical: 0 High: 0 Medium: 0 Low: 0 Info: 12

b. Bật Wireshark sau đó tiến hành quét và xác định các bước mà Nessus đã thực hiện để hoàn tất quá trình quét.

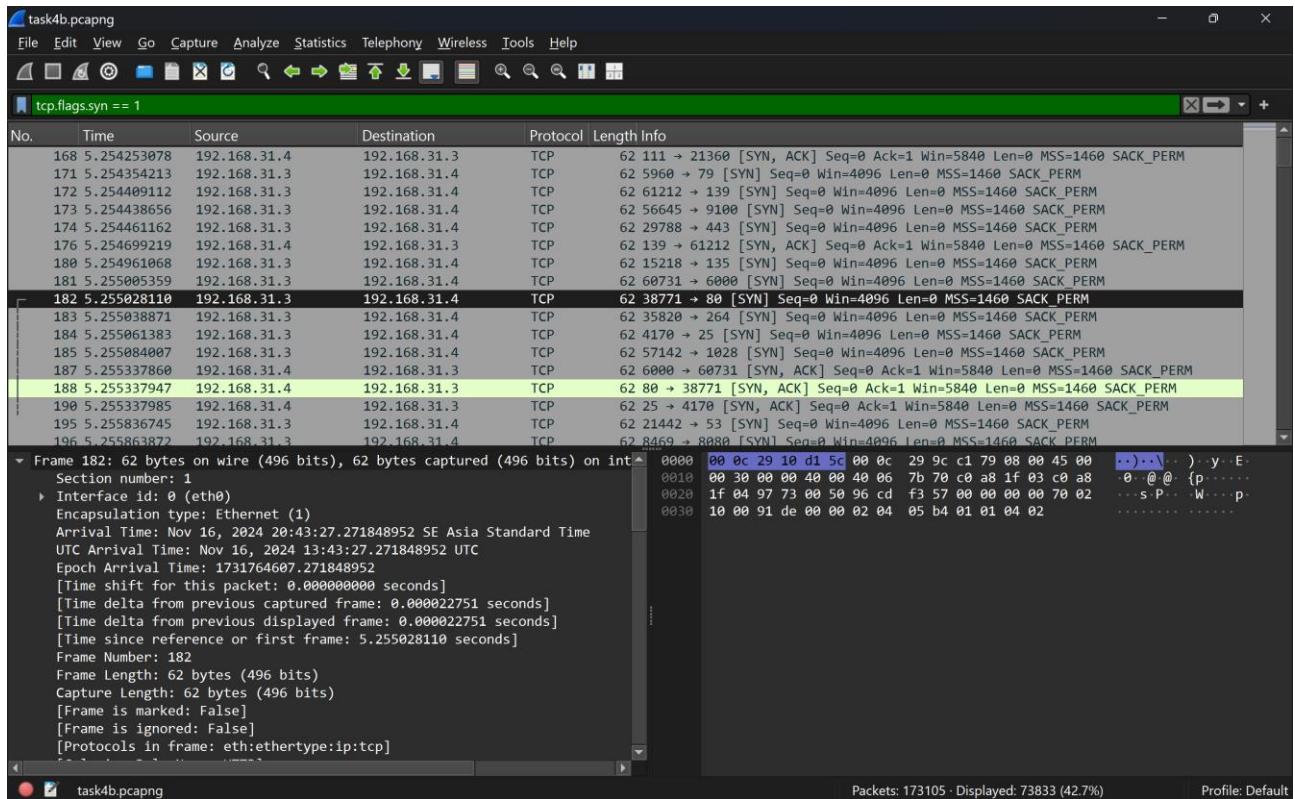
- Quy trình quét Nessus trên hệ thống IP 192.168.31.4:

+ Nessus gửi gói ICMP echo request nhằm mục đích kiểm tra xem máy đích có đang hoạt động hay không. Nếu máy đích trả lời bằng gói ICMP echo reply, Nessus xác định rằng máy đích đang sống và có thể tiếp tục các bước quét tiếp theo.



+ Sau khi xác nhận máy đích sống, Nessus gửi các gói TCP SYN đến các cổng phổ biến trên máy đích (ví dụ: 22, 25, 80, 443, ...). Gói TCP SYN được gửi đến các cổng để kiểm tra xem cổng đó có mở không.

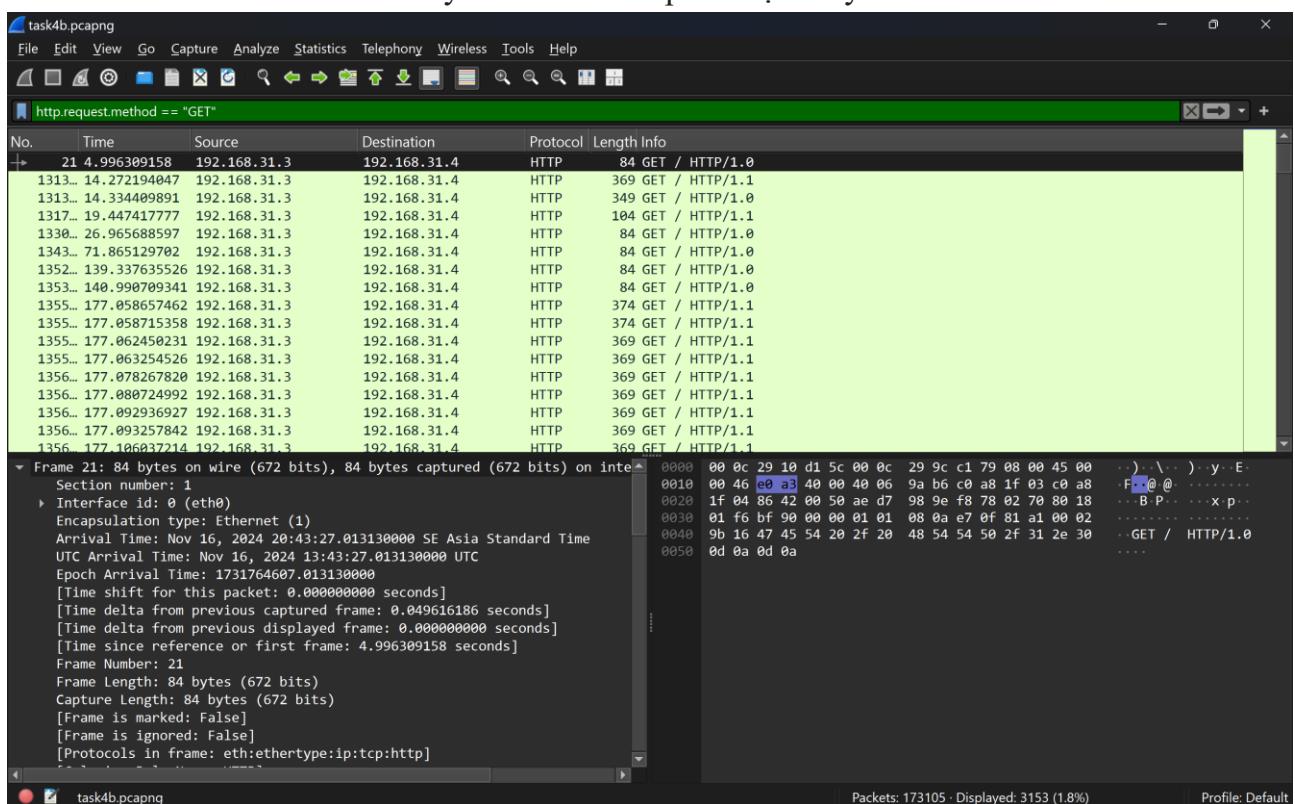
- Nếu cổng mở, máy đích sẽ phản hồi bằng một gói **SYN-ACK**, cho biết cổng có thể kết nối.
- Nếu cổng đóng, máy đích sẽ phản hồi bằng gói **RST**, thông báo rằng cổng không chấp nhận kết nối.



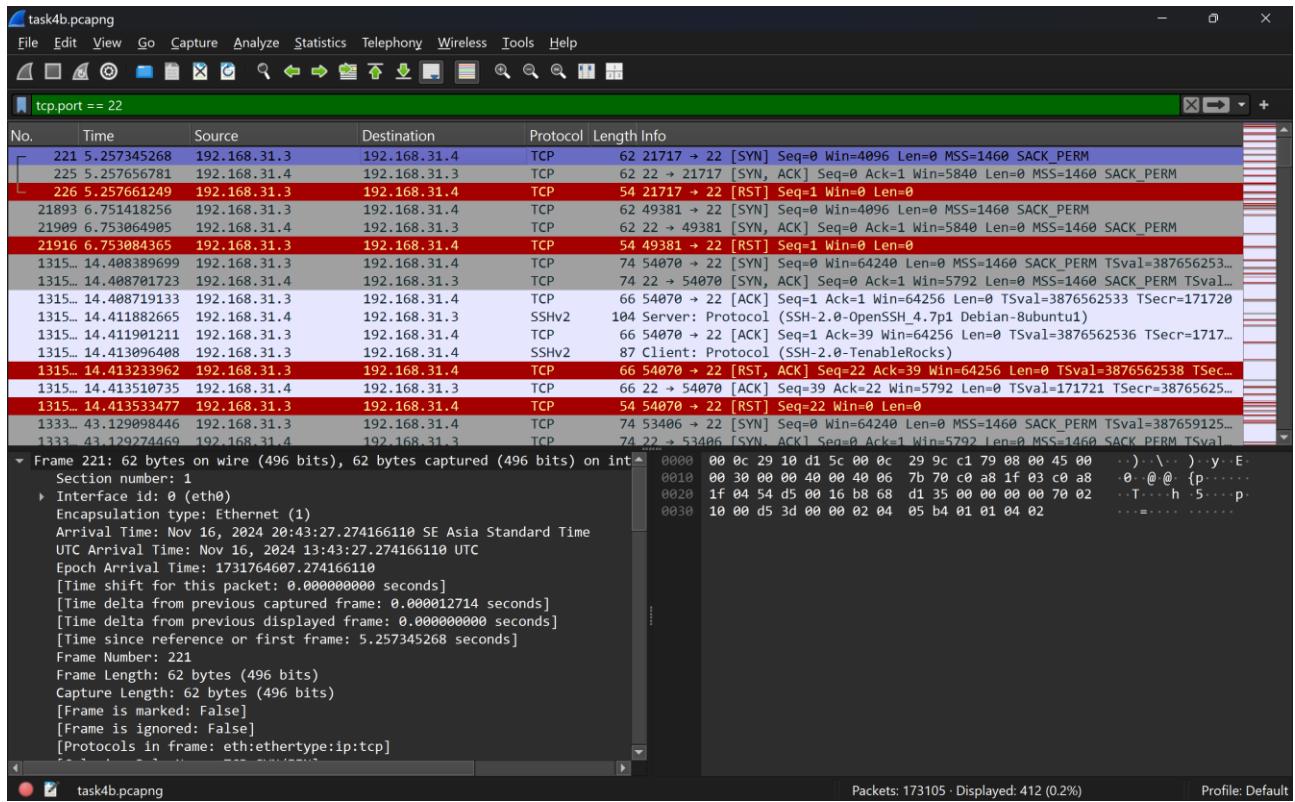
+ Khi xác định được các cổng mở, Nessus gửi các gói tin để kiểm tra thông tin dịch vụ và phiên bản chạy trên cổng đó.

- **Ví dụ:**

- Gửi truy vấn HTTP để phát hiện máy chủ web.



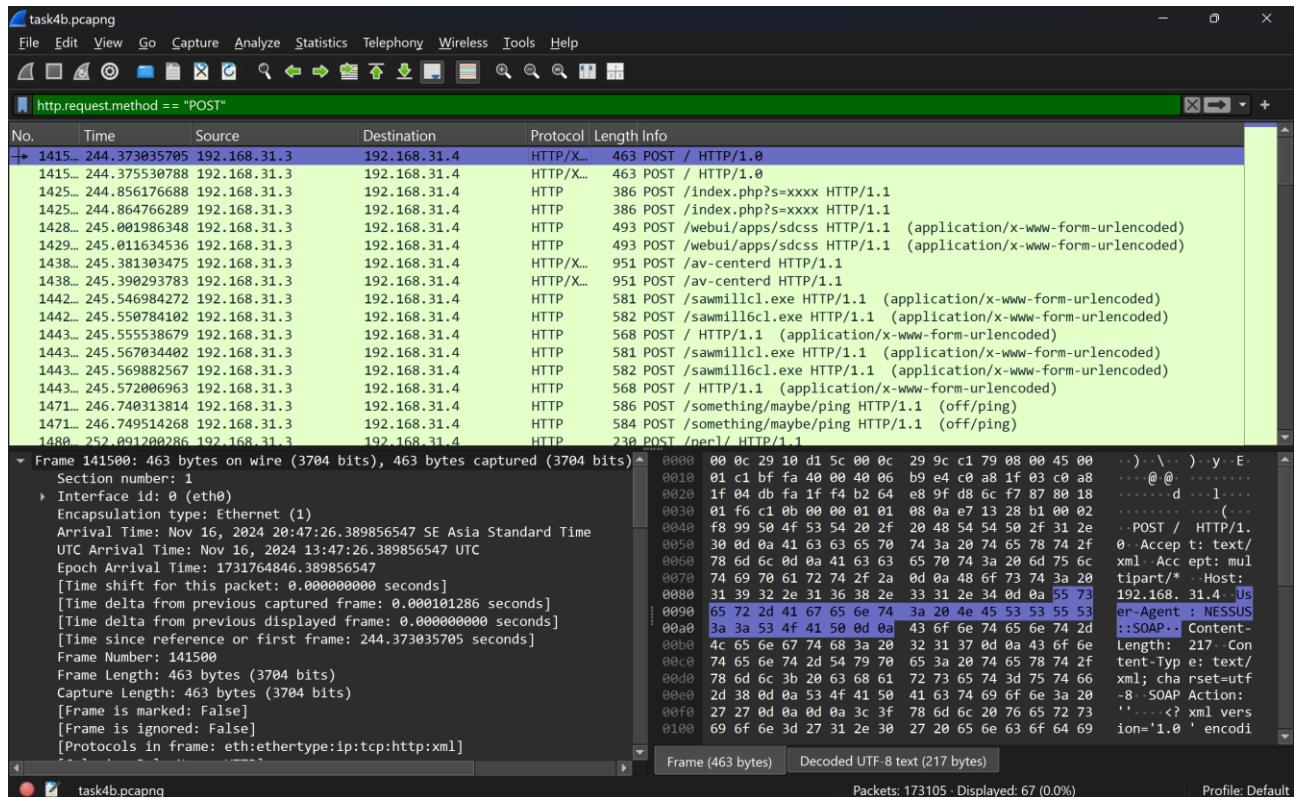
- Gửi gói tin SSH Handshake để phát hiện dịch vụ SSH.



+ Sau khi xác định dịch vụ, Nessus sẽ kiểm tra các lỗ hổng bảo mật bằng cách gửi các tải trọng độc hại hoặc các truy vấn đặc biệt.

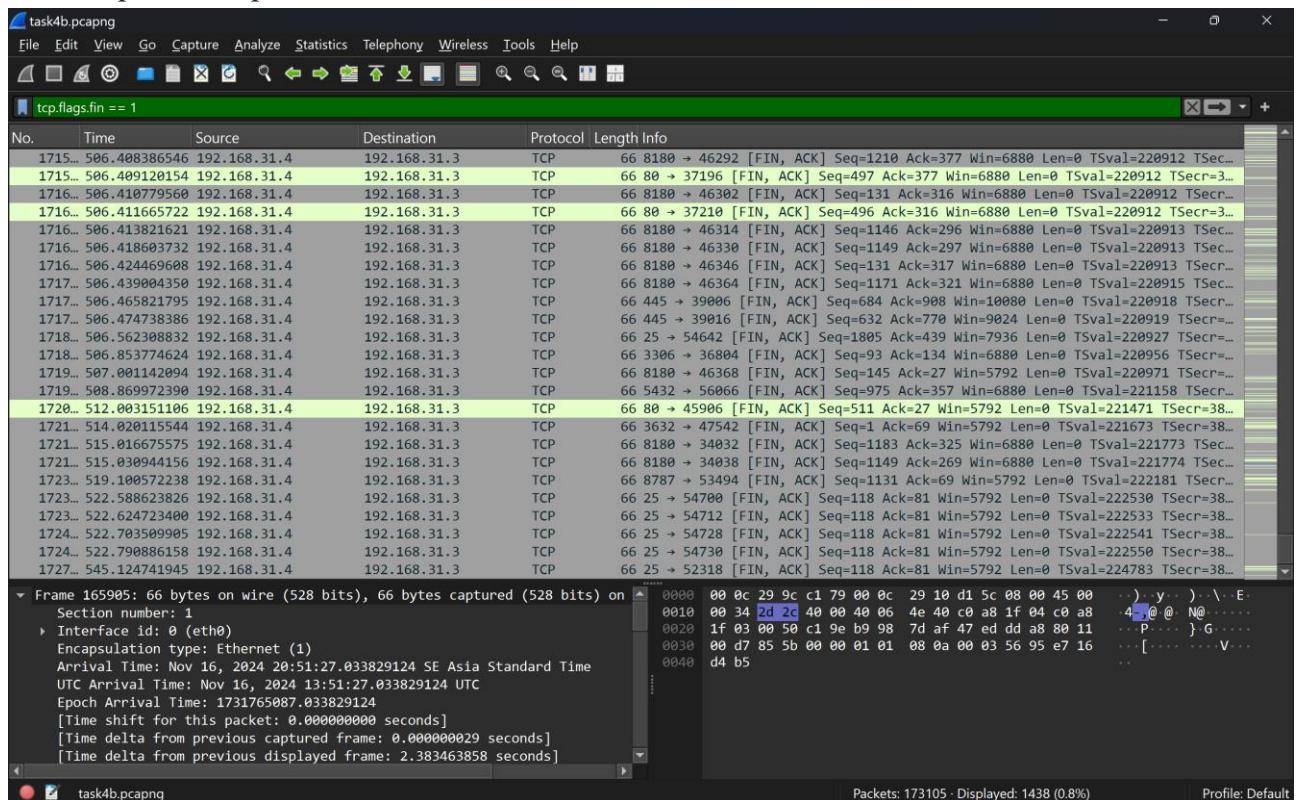
- Nessus có thể gửi các yêu cầu HTTP độc hại hoặc các truy vấn đặc biệt để kiểm tra các lỗ hổng.
 - Ta có thể tìm thấy các gói HTTP POST với dữ liệu độc hại được gửi tới các công dịch vụ.

Lab 03: Gather information & Vulnerability Scanning



- Nessus so sánh phiên bản dịch vụ với cơ sở dữ liệu lỗ hổng đã biết để xác định các lỗ hổng đã được biết đến.

+ Sau khi quét xong, Nessus tổng hợp kết quả và báo cáo. Quá trình này không tạo ra gói tin mới. Ta có thể thấy một số gói tin TCP FIN hoặc ICMP Destination Unreachable khi quá trình quét kết thúc.



c. Quét lại những quét thêm port UDP

Metasploitable2 - Basic

[Back to My Scans](#)

Hosts	Vulnerabilities	Remediations	History
1	70	3	1 History

Start Time ▾ Last Scanned Status Scan Details

Current Today at 8:43 AM	Today at 8:52 AM	Completed	X
--------------------------	------------------	-----------	---

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 8:43 AM
End: Today at 8:52 AM
Elapsed: 9 minutes

Vulnerabilities

Critical
High
Medium
Low
Info

Metasploitable2 - Basic / 192.168.31.4

[Back to Hosts](#)

Vulnerabilities 11							
Filter	Search Vulnerabilities	Count	Host Details				
Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▾	Family ▾	Count ▾	IP: 192.168.31.4 MAC: 00:0C:29:10:D1:5C OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy) Start: Today at 9:01 AM End: Today at 9:10 AM Elapsed: 10 minutes KB: Download
Critical	10.0 *	5.1	0.1175	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	Gain a shell remotely	2	
Critical	10.0 *	5.1	0.1175	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Gain a shell remotely	1	
Critical	9.8	9.0	0.9737	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	
High	8.6	5.2	0.0164	ISC BIND Service Downgrade / Reflected DoS	DNS	1	
High	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	1	
High	7.5 *	5.9	0.015	rsh Service Detection	Service detection	1	
Medium	6.8	6.0	0.1395	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	DNS	1	
Medium	5.9	4.4	0.9717	ISC BIND Denial of Service	DNS	1	
Medium	5.3			SMB Signing not required	Misc.	1	
Medium	4.0 *	7.3	0.0114	SMTP Service STARTTLS Plaintext Command Injection	SMTP problems	1	
Low	3.4	5.1	0.9749	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	General	2	

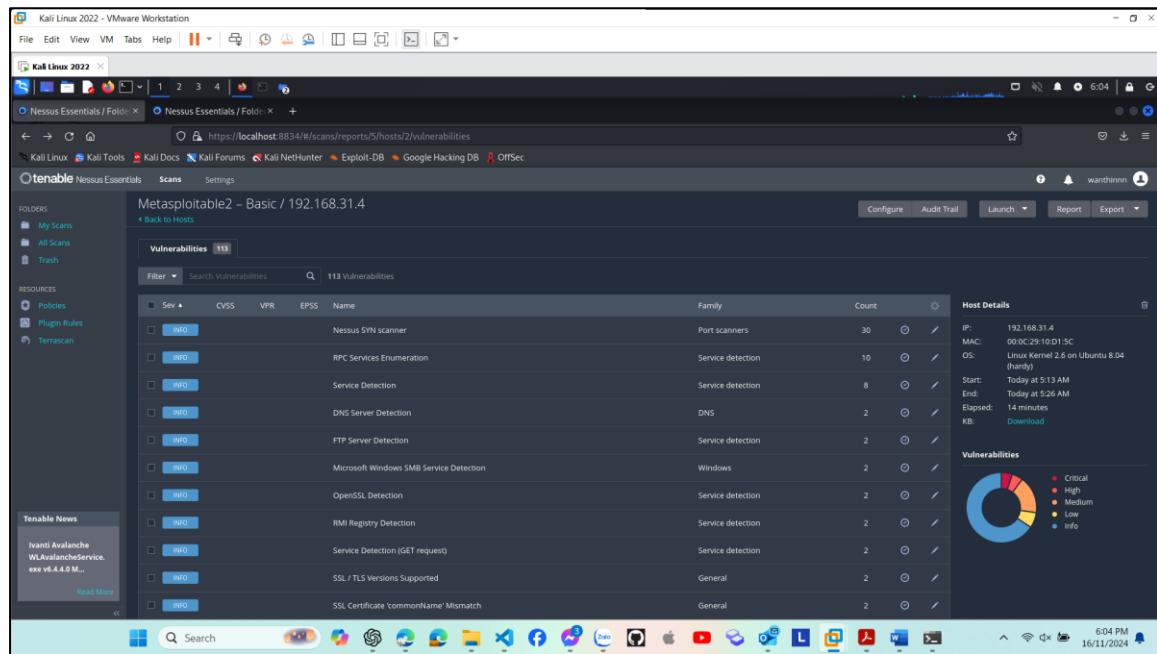
Vulnerabilities

Critical
High
Medium
Low
Info

Task 15: Thực hiện lại các bước trên để quét máy Metasploitable 2 có sử dụng tài khoản chứng thực. Kiểm tra kết quả quét và so sánh với việc quét không sử dụng tài khoản chứng thực. Hãy liệt kê các ưu, nhược điểm khi quét có tài khoản chứng thực và không có tài khoản chứng thực.

Trả lời:

* Kết quả quét khi không sử dụng tài khoản chứng thực:



- Kiểm tra kết quả:

+ Các thông tin được quét sẽ chủ yếu dựa vào các dịch vụ mở và thông tin banner mà Nessus thu thập được.

+ Các lỗi được phát hiện có thể không đầy đủ do thiếu quyền truy cập vào hệ thống.

- Tạo lưu kết quả quét vào file "basic_khong-chung-thuc.txt":

+ Thông tin giới hạn hơn:

- Dựa vào banner của các dịch vụ mở (ví dụ: HTTP, SSH, FTP) nhưng thiếu thông tin chi tiết như phiên bản phần mềm hoặc lỗ hổng cụ thể.
- Chỉ phát hiện được các dịch vụ và cổng đang hoạt động:
 - DNS (UDP/53), FTP (TCP/21), SMB (TCP/139), HTTP (TCP/80).
- Các lỗ hổng được phát hiện chủ yếu là bề mặt (CVSS thấp liên quan đến thông tin banner).

+ Không thu thập thông tin hệ điều hành đầy đủ: Chỉ ghi nhận tên OS là **Linux Kernel 2.6** trên **Ubuntu 8.04**, không có thông tin chi tiết về bản build.

```

result.txt          result_ok.txt          auth_chung-thuc.txt          basic_khong_chung-thuc.txt
File Edit View
1731752824 3 Launched/108659+282891
1731752824 3 Launched/33942+237571
1731752824 3 Launched/14291+237000
1731752824 3 Launched/81919+235368
1731752824 3 Launched/78602+234050
1731752824 3 Launched/16274+228721
1731752824 3 Launched/122614+123102
1731752824 3 Launched/11341+29434
1731752824 3 Launched/15659+24176
1731752824 3 Launched/33439+452390
1731752824 3 Launched/11691+440062
1731752824 3 Launched/166370+438990
1731752824 3 Launched/10239+438942
1731752824 3 Launched/201388+438463
1731752824 1 Host/normalization/original_os=Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
1731752824 3 Launched/22466+294348
1731752824 3 Launched/11341+294303
1731752824 3 Launched/11341+29434
1731752824 3 Launched/15659+24176
1731752824 3 Launched/33439+452390
1731752824 3 Launched/11691+440062
1731752824 3 Launched/166370+438990
1731752824 3 Launched/10239+438942
1731752824 3 Launched/201388+438463
1731752824 Host/normalization/original_os=Linux Kernel 2.6 on Ubuntu 8.04
1731752824 3 Launched/22466+294348
1731752824 3 Launched/11341+294303
1731752824 3 Launched/11341+29434
1731752824 3 www/apache/0/backported=1
1731752824 3 Launched/15643+235153
1731752824 3 Launched/109382+233093
1731752824 3 Launched/13841+232332
1731752824 3 Launched/11239+231982
1731752824 3 Launched/20834+87302
1731752824 SYNScanner/cnxTime/8180=0
1731752824 3 Ports/tcp/2121=1
1731752824 3 Launched/104378+439070
1731752824 3 Launched/11341+294303
1731752824 3 Launched/11341+29434
1731752824 3 Launched/171347+438189
1731752824 3 Launched/190512+390107
1731752824 3 Launched/11205+320109
1731752824 3 Launched/11519+234434
1731752824 3 Launched/22319+228711
1731752824 3 Launched/11897+228709
1731752824 1 vnc/banner/5900=RFB 003.003\n
1731752824 3 Launched/35559+87299
1731752824 3 Launched/192768+34415
1731752824 3 Launched/11341+294303
1731752824 3 Launched/10640+23416
1731752824 1 Plugins/CVS/8915+CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N
1731752824 3 Launched/10498+355657

```

+ Thiếu thông tin cấu hình chi tiết: Không phát hiện được thông tin về socket Unix hoặc cấu hình dịch vụ cụ thể (PostgreSQL Client, Apache Log4j).

```

result.txt          result_ok.txt          auth_chung-thuc.txt          basic_khong_chung-thuc.txt
File Edit View
1731752824 3 Launched/108659+282891
1731752824 3 Launched/33942+237571
1731752824 3 Launched/14291+237000
1731752824 3 Launched/81919+235368
1731752824 3 Launched/78602+234050
1731752824 3 Launched/16274+228721
1731752824 3 Launched/122614+123102
1731752824 3 Launched/11341+29434
1731752824 3 Launched/15659+24176
1731752824 3 Launched/33439+452390
1731752824 3 Launched/11691+440062
1731752824 3 Launched/166370+438990
1731752824 3 Launched/10239+438942
1731752824 3 Launched/201388+438463
1731752824 Host/normalization/original_os=Linux Kernel 2.6 on Ubuntu 8.04
1731752824 3 Launched/22466+294348
1731752824 3 Launched/11341+294303
1731752824 3 Launched/11341+29434
1731752824 3 www/apache/0/backported=1
1731752824 3 Launched/15643+235153
1731752824 3 Launched/109382+233093
1731752824 3 Launched/13841+232332
1731752824 3 Launched/11239+231982
1731752824 3 Launched/20834+87302
1731752824 SYNScanner/cnxTime/8180=0
1731752824 3 Ports/tcp/2121=1
1731752824 3 Launched/104378+439070
1731752824 3 Launched/11341+294303
1731752824 3 Launched/11341+29434
1731752824 3 Launched/171347+438189
1731752824 3 Launched/190512+390107
1731752824 3 Launched/11205+320109
1731752824 3 Launched/11519+234434
1731752824 3 Launched/22319+228711
1731752824 3 Launched/11897+228709
1731752824 1 vnc/banner/5900=RFB 003.003\n
1731752824 3 Launched/35559+87299
1731752824 3 Launched/192768+34415
1731752824 3 Launched/11341+294303
1731752824 3 Launched/10640+23416
1731752824 1 Plugins/CVS/8915+CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N
1731752824 3 Launched/10498+355657

```

Notepad
Cannot find "PostgreSQL Client"

OK

```

result.txt          result_ok.txt          auth_chung-thuc.txt          basic_khong_chung-thuc.txt
File Edit View
1731752824 3 Launched/108659+282891
1731752824 3 Launched/33942+237571
1731752824 3 Launched/14291+237000
1731752824 3 Launched/81919+235368
1731752824 3 Launched/78602+234050
1731752824 3 Launched/16274+228721
1731752824 3 Launched/122614+123102
1731752824 3 Launched/11341+29434
1731752824 3 Launched/15659+24176
1731752824 3 Launched/33439+452390
1731752824 3 Launched/11691+440062
1731752824 3 Launched/166370+438990
1731752824 3 Launched/10239+438942
1731752824 3 Launched/201388+438463
1731752824 Host/normalization/original_os=Linux Kernel 2.6 on Ubuntu 8.04
1731752824 3 Launched/22466+294348
1731752824 3 Launched/11341+294303
1731752824 3 Launched/11341+29434
1731752824 3 Launched/171347+438189
1731752824 3 Launched/190512+390107
1731752824 3 Launched/11205+320109
1731752824 3 Launched/11519+234434
1731752824 3 Launched/22319+228711
1731752824 3 Launched/11897+228709
1731752824 1 vnc/banner/5900=RFB 003.003\n
1731752824 3 Launched/35559+87299
1731752824 3 Launched/192768+34415
1731752824 3 Launched/11341+294303
1731752824 3 Launched/10640+23416
1731752824 1 Plugins/CVS/8915+CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N
1731752824 3 Launched/10498+355657

```

Notepad
Cannot find "Apache Log4j"

OK

* Kết quả quét khi sử dụng tài khoản chứng thực:

The screenshot shows the Nessus interface on a Kali Linux host. The main window displays a scan report for 'Metasploitable2 - Auth / 192.168.31.4'. The 'Vulnerabilities' tab is selected, showing 245 entries. The results are filtered by severity: Info (the majority), Low, Medium, High, and Critical. The left sidebar shows navigation links like 'Tenable News' and 'Scan Details'. The right sidebar provides 'Host Details' including IP, MAC, OS, Start/End times, and Elapsed duration.

- Kiểm tra kết quả: chi tiết hơn, bao gồm:

- + Các lỗ hổng từ cấp hệ điều hành.
- + Các bản vá bị thiếu.
- + Cấu hình yếu (weak configurations) trong hệ thống.

- Tải lưu kết quả quét vào file "auth_chung-thuc.txt", phân tích:

- + Thông tin chi tiết hơn:
 - o Các bản ghi từ hệ điều hành (OS) được phát hiện: **Linux Kernel 2.6.24-16-server trên Ubuntu 8.04.**

```
result.txt          result_ok.txt          auth_chung-thuc.txt          basic_khong-chung-thuc.txt
File Edit View
1731753849 3 Launched/210774-433672
1731753849 3 Launched/65115-433622
1731753849 3 Launched/183165-432698
1731753849 3 Launched/164287-432642
1731753849 3 Launched/187954-432457
1731753849 3 Launched/204925-432393
1731753849 1 Host/uname=linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux\n
1731753849 3 Launched/33942-206472
1731753849 3 Launched/108659-182647
1731753849 3 Launched/122614-27029
1731753849 3 Launched/192845-26426
1731753849 3 Launched/166370-439938
1731753849 1 Host/normalization/original_os=linux Kernel 2.6.24-16-server on Ubuntu 8.04
```

- o Phát hiện các dịch vụ chạy trên cổng như:
 - SSH (TCP/22).
 - MySQL (TCP/3306).
 - FTP (TCP/21).
 - VNC (TCP/5900).

- Phát hiện các lỗ hổng liên quan đến cấu hình sai hoặc phần mềm lỗi thời, ví dụ: Apache Log4j, PostgreSQL Client.

The screenshot displays two terminal windows side-by-side within Visual Studio Code. Both windows show log entries from a file named 'auth_chung-thuc.txt'.

Left Terminal (Apache Log4j):

```

auth_chung-thuc.txt
145 1/34/2024 3 Launched/142204=43402
169 1731753849 3 Launched/147989=434406
170 1731753849 3 Launched/151836=434364
171 1731753849 3 Launched/28106=434362
172 1731753849 3 Launched/153925=434336
173 1731753849 3 Launched/28127=434294
174 1731753849 3 Launched/161663=434249
175 1731753849 3 Launched/31783=434156
176 1731753849 3 Launched/177111=434088
177 1731753849 3 Launched/182529=433980
178 1731753849 3 Launched/209439=433700
179 1731753849 3 Launched/28716=433116
180 1731753849 3 Launched/45487=433047
181 1731753849 3 Launched/49303=432885
182 1731753849 3 Launched/183738=432776
183 1731753849 3 Launched/183128=432632
184 1731753849 3 Launched/168479=432605
185 1731753849 3 Launched/183410=432538
186 1731753849 3 Launched/207439=432375
187 1731753849 1 vnc/banner/5900=RFB 003.003\n
188 1731753849 3 Launched/192768=26488
189 1731753849 3 Launched/44048=18207
190 1731753849 3 Launched/186662=16178
191 1731753849 1 installed/sw/Apache Log4j/L3Vzc19zaGFyZS9qYXZhL2xvzzRqLTEuMi4xNS5qYXIS/JdbcAppender.class association=Found
192 1731753849 1 Host/ifconfig/mac_addr=00:0c:29:10:d1:66
193 1731753849 3 Host/ifconfig/mac_addr=00:0c:29:10:d1:5c
194 1731753849 3 Launched/66171=437486
195 1731753849 3 Launched/83180=437488
196 1731753849 3 Launched/104322=437268
197 1731753849 3 Launched/108834=437254
198 1731753849 3 Launched/133800=437193
199 1731753849 3 Launched/165286=437101
200 1731753849 3 Launched/182612=436987
201 1731753849 3 Launched/203921=436873
202 1731753849 3 Launched/207226=436533
203 1731753849 3 Launched/56089=435954
204 1731753849 3 Launched/56384=435934

```

Right Terminal (PostgreSQL Client):

```

auth_chung-thuc.txt
200 1731753849 3 Launched/100353=435530
284 1731753849 3 Launched/200488=433777
285 1731753849 3 Launched/37362=433707
286 1731753849 3 Launched/39491=433485
287 1731753849 3 Launched/40329=433433
288 1731753849 3 Launched/151451=432740
289 1731753849 3 Launched/163863=432644
290 1731753849 1 HostLevelChecks/cred_type=password
291 1731753849 1 mysql/3306/ver=5.0.51a-3ubuntu5
292 1731753849 3 mysql/3306/port=3306
293 1731753849 3 Launched/11149=205859
294 1731753849 3 Success/42088=1
295 1731753849 3 Launched/10280=179279
296 1731753849 1 Services/telnet/banner/23=
297 1731753849 3 Launched/10906=26346
298 1731753849 1 Known/tcp/2049=rpc-nfs
299 1731753849 3 Launched/10308=16079
300 1731753849 1 Errors/mysql_5_6_41.nasl/0>Error parsing version: "5.0.51a-3ubuntu5" at index: 7: invalid character in version string
301 1731753849 3 Launched/145251=439491
302 1731753849 1 installed/sw/PostgreSQL client/L3Vzc19saIIVccG9zdGdyZXNxbC84LjMvYml3BzClwgkHZpYSBWYWRwdlG1hbmfNzXIp/cpe/v22C=cpe:/a:post
303 1731753849 3 Launched/52499=437584
304 1731753849 3 Launched/59034=437528
305 1731753849 3 Success/59292=1
306 1731753849 3 Launched/72572=437459
307 1731753849 3 Launched/72899=437455
308 1731753849 3 Launched/80028=437425
309 1731753849 3 Launched/87470=437375
310 1731753849 3 Launched/110406=437249
311 1731753849 3 Launched/147978=437167
312 1731753849 3 Launched/154274=437143
313 1731753849 3 Launched/173443=437062
314 1731753849 3 Launched/180510=437006
315 1731753849 3 Launched/183454=436981
316 1731753849 3 Launched/187657=436967
317 1731753849 3 Launched/143478=436530
318 1731753849 3 Launched/55921=435960
319 1731753849 3 Launched/57763=435861

```

- Liệt kê đầy đủ các socket hoạt động (TCP và Unix domain sockets).

+ Thông tin dịch vụ:

- Phát hiện thông tin từ banner của các dịch vụ (VD: phiên bản cụ thể của VNC: RFB 003.003).

The screenshot shows a NetworkMiner capture of an RFB session. The session details pane shows the session ID as RFB 003.003, with 1 of 2 frames. The list of frames shows numerous frames from host 173.17.53.849, mostly labeled as "Launched". Frame 187 is highlighted in yellow and shows the command "1731753849 1 vnc/banner/:5900-RFB 003.003\n".

- Lấy thông tin từ ifconfig (địa chỉ MAC của các interface: 00:0C:29:10:D1:66, 00:0C:29:10:D1:5C).

The screenshot shows a NetworkMiner capture of an ifconfig session. The session details pane shows the session ID as 00:0C:29:10:D1:66, with 1 of 7 frames. The list of frames shows numerous frames from host 173.17.53.849, mostly labeled as "Launched". Frame 192 is highlighted in yellow and shows the command "1731753849 1 Host/ifconfig/mac_addr=00:0C:29:10:D1:66".

- Cấu hình của từng dịch vụ: Ports/tcp/6697=1 (dịch vụ IRC trên cổng 6697).

The screenshot shows a NetworkMiner capture of a ports/tcp/6697=1 session. The session details pane shows the session ID as Ports/tcp/6697=1, with 1 of 3 frames. The list of frames shows numerous frames from host 173.17.53.849, mostly labeled as "Launched". Frame 329 is highlighted in yellow and shows the command "1731753849 3 Ports/tcp/6697=1".

+ Các lỗi cấu hình sâu: Phát hiện các vấn đề trong cấu hình như:

- Cleartext credentials** cho các dịch vụ như RLOGIN hoặc FTP.
- Lỗi bảo mật SSL/TLS cho các dịch vụ hỗ trợ STARTTLS.

+ Thông tin tài khoản: Phát hiện tài khoản **root** và mật khẩu mặc định (msfadmin).

The screenshot shows a NetworkMiner capture of an msfadmin session. The session details pane shows the session ID as msfadmin, with 1 of 16 frames. The list of frames shows frame 1440, which is highlighted in yellow and contains the command "1440 trusted network!\n\nContact: msfdev[at]metasploit.com\n\nlogin with msfadmin/msfadmin to get started\n\n\n<pre>\n<a href=\"/twi...".

* So sánh quét có và không có tài khoản chứng thực

Tiêu chí	Quét không chứng thực	Quét có chứng thực
Phạm vi phát hiện	Hạn chế, chỉ dựa vào banner và dịch vụ mở.	Toàn diện, bao gồm thông tin hệ điều hành, cấu hình, và phần mềm.
Thông tin hệ điều hành	Chỉ phát hiện được tên OS và đôi khi phiên bản kernel.	Phát hiện đầy đủ tên OS, phiên bản, kernel, bản vá thiếu và cấu hình OS.
Dịch vụ phát hiện	Dựa vào banner của dịch vụ (ví dụ: FTP, HTTP, SSH).	Thông tin chi tiết từng dịch vụ, bao gồm cấu hình sâu và phiên bản.
Lỗ hổng dịch vụ	Chỉ phát hiện lỗ hổng công khai liên quan đến dịch vụ.	Phát hiện cả lỗ hổng phần mềm nội bộ và cấu hình sai của dịch vụ.
Cấu hình hệ thống	Không kiểm tra được cấu hình nội bộ hoặc quyền hạn trên hệ thống.	Có thể phát hiện cấu hình yếu, quyền hạn thừa, hoặc thư mục dễ bị truy cập.
Thông tin tài khoản	Không phát hiện được thông tin liên quan đến tài khoản.	Phát hiện mật khẩu mặc định, thông tin đăng nhập lưu dưới dạng plaintext.
Bảo mật SSL/TLS	Chỉ kiểm tra bè mặt (ví dụ: mã hóa yếu hoặc lỗi chứng chỉ).	Kiểm tra đầy đủ cấu hình SSL/TLS, lỗi chuỗi chứng chỉ, chứng chỉ tự ký,...
Khả năng kiểm tra bản vá	Không phát hiện được các bản vá thiếu.	Phát hiện chi tiết các bản vá còn thiếu cho hệ điều hành và phần mềm.
Hiệu suất quét	Nhanh hơn, vì chỉ quét bè mặt và các dịch vụ mở.	Chậm hơn do cần truy cập và phân tích hệ thống từ bên trong.
Yêu cầu	Không cần thông tin đăng nhập, phù hợp với quét mạng mở.	Yêu cầu tài khoản hợp lệ với quyền truy cập đủ (user hoặc root).

* Phân tích ưu, nhược điểm

- Quét không chứng thực:

+ Ưu điểm:

- Dễ thực hiện: Không cần thông tin đăng nhập hoặc quyền truy cập hệ thống.
- Nhanh chóng: Quét chỉ tập trung vào dịch vụ mở và giao diện mạng.
- Phù hợp cho reconnaissance (dò quét sơ bộ): Thích hợp để thu thập thông tin ban đầu hoặc kiểm tra phạm vi mạng.

+ Nhược điểm:

- Thông tin hạn chế: Không thể phát hiện lỗi bên trong hoặc cấu hình sai trong hệ thống.

- Không chính xác: Kết quả phụ thuộc vào thông tin public như banner hoặc phản hồi của dịch vụ.
- Không phát hiện bản vá hoặc cấu hình hệ điều hành.

- Quét có chứng thực

+ Ưu điểm:

- Chi tiết và toàn diện: Phát hiện lỗi từ dịch vụ, hệ điều hành, đến cấu hình sâu.
- Xác định rõ nguyên nhân lỗi hỏng: Giúp đề xuất biện pháp khắc phục cụ thể.
- Tích hợp kiểm tra bản vá: Phát hiện các bản vá bị thiếu và lỗi cấu hình phần mềm.

+ Nhược điểm:

- Phụ thuộc vào tài khoản: Yêu cầu tài khoản hợp lệ với quyền truy cập phù hợp.
- Dễ bị hạn chế: Nếu tài khoản bị khóa hoặc không đủ quyền, kết quả quét sẽ không đầy đủ.
- Thời gian quét dài hơn: Do phân tích chi tiết từng thành phần trong hệ thống.

Task 16:

- Thực hiện lại các bước ở trên để quét máy Metasploitable 2 sử dụng plugin NFS Exported Share Information Disclosure.
- Chạy Wireshark hoặc tcpdump trong suốt quá trình scan sử dụng 1 plugin duy nhất. Liệt kê các port khác mà Nessus thực hiện scan, mà không phải port 111? Tại sao Nessus lại scan các port khác, trong khi chúng ta đã chỉ định chỉ scan duy nhất 1 port là 111?
- Mô tả cách làm để ngăn chặn việc Nessus scan port khác không phải là port được chỉ định
- Thực hiện quét lại sử dụng 2 plugin khác.

Trả lời:

- Thực hiện lại các bước ở trên để quét máy Metasploitable 2 sử dụng plugin NFS Exported Share Information Disclosure.

- Kết quả sau khi quét bằng plugin NFS Exported Share Information Disclosure:

Vulnerability	Severity	Family	Count
Nessus Scan Information	Info	Settings	1
Nessus SYN scanner	Info	Port scanners	1

b. Chạy Wireshark hoặc tcpdump trong suốt quá trình scan sử dụng 1 plugin duy nhất. Liệt kê các port khác mà Nessus thực hiện scan, mà không phải port 111? Tại sao Nessus lại scan các port khác, trong khi chúng ta đã chỉ định chỉ scan duy nhất 1 port là 111?

- Sử dụng từ khóa (ip.addr == 192.168.137.129) && !(tcp.port == 111) để loại trừ port 111 và chỉ hiển thị các gói tin liên quan đến địa chỉ IP của máy Metasploitable 2:

No.	Time	Source	Destination	Protocol	Length	Info
214	3.350897267	192.168.137.129	192.168.137.128	TCP	74	139 - 42696 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TStamp=26442
217	3.350940186	192.168.137.128	192.168.137.129	TCP	66	42696 - 139 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TStamp=4092156296 TSectr=26442
219	3.351392164	192.168.137.128	192.168.137.129	NBSS	138	Session request, to Nessus582932<20> from <20>
221	3.352017884	192.168.137.129	192.168.137.128	TCP	66	139 - 42696 [ACK] Seq=1 Ack=73 Win=5792 Len=0 TStamp=26442 TSectr=4092156297
222	3.352627615	192.168.137.129	192.168.137.128	NBSS	70	Positive session response
223	3.352644330	192.168.137.128	192.168.137.129	TCP	66	42696 - 139 [ACK] Seq=73 Ack=5 Win=32128 Len=0 TStamp=4092156298 TSectr=26442
224	3.353374246	192.168.137.128	192.168.137.129	TCP	66	42696 - 139 [RST, ACK] Seq=73 Ack=5 Win=32128 Len=0 TStamp=4092156299 TSectr=26442
225	3.354619169	192.168.137.128	192.168.137.129	Portmap	82	V2 DUMP Call (Reply In 229)
226	3.355036403	192.168.137.128	192.168.137.129	TCP	74	51184 - 139 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TStamp=4092156300 TSectr=26443
227	3.355265236	192.168.137.129	192.168.137.128	TCP	60	135 - 51184 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
228	3.355843403	192.168.137.128	192.168.137.129	TCP	74	40692 - 445 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TStamp=4092156301 TSectr=26443
229	3.356160906	192.168.137.129	192.168.137.128	Portmap	510	V2 DUMP Reply (Call In 225)
230	3.356161078	192.168.137.129	192.168.137.128	TCP	74	445 - 40692 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TStamp=26443
231	3.356210379	192.168.137.128	192.168.137.129	TCP	66	40692 - 445 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TStamp=4092156302 TSectr=26443
232	3.362504472	192.168.137.128	192.168.137.129	SMB	241	Negotiate Protocol Request
233	3.363661361	192.168.137.129	192.168.137.128	TCP	66	445 - 40692 [ACK] Seq=1 Ack=176 Win=6880 Len=0 TStamp=26444 TSectr=4092156308
234	3.363661684	192.168.137.129	192.168.137.128	SMB	197	Negotiate Protocol Response
235	3.363713461	192.168.137.128	192.168.137.129	TCP	66	40692 - 445 [ACK] Seq=176 Ack=132 Win=32000 Len=0 TStamp=4092156309 TSectr=26444
236	3.368070450	192.168.137.128	192.168.137.129	SMB	306	Session Setup AndX Request, NTLMSSP_NEGOTIATE
237	3.368195732	192.168.137.128	192.168.137.129	SNMP	85	get-next-request 1.3.6.1.2.1.1.1.0
238	3.369011022	192.168.137.129	192.168.137.128	ICMP	113	Destination unreachable (Port unreachable)
239	3.369487460	192.168.137.129	192.168.137.128	SMB	440	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED

+ Các port mà nessus scan gồm rất nhiều port khác nhau như 139,135,445....

- Lý do: Nessus quét thêm các cổng khác để tìm kiếm các dịch vụ liên quan hoặc phụ thuộc đến mục tiêu. Điều này giúp tăng cường khả năng phát hiện các lỗ hổng tiềm ẩn, đặc biệt trong các dịch vụ liên quan đến NFS

c. Mô tả cách làm để ngăn chặn việc Nessus scan port khác không phải là port được chỉ định

Để ngăn Nessus quét các cổng không mong muốn:

- Cấu hình policy trong Nessus:

+ Vào Scan Settings

+ Ở mục Port Scanning, chọn Custom Ports

+ Chỉ định duy nhất port 111 (hoặc port mong muốn).

- Vô hiệu hóa việc scan các cổng không liên quan: Trong phần Discovery, tắt các mục tự động phát hiện (Service Detection).

d. Thực hiện quét lại sử dụng 2 plugin khác.

- Plugin RPC Portmapper Service Detection: là một plugin được thiết kế để phát hiện dịch vụ Portmapper (RPC Port Mapper) đang chạy trên một máy chủ. Portmapper là một dịch vụ quan trọng trong giao thức Remote Procedure Call (RPC), giúp ánh xạ các dịch vụ RPC với các cổng mạng cụ thể để các ứng dụng có thể tìm thấy và kết nối đến các dịch vụ đó.

The screenshot shows the Tenable Nessus Essentials interface. On the left sidebar, there are sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Terrascan), and Tenable News. The main content area displays four sections of scan results:

- Port 5900/tcp was found to be open**: Hosts: 5900/tcp → 192.168.137.129
- Port 6000/tcp was found to be open**: Hosts: 6000/tcp → 192.168.137.129
- Port 6667/tcp was found to be open**: Hosts: 6667/tcp → 192.168.137.129
- Port 8009/tcp was found to be open**: Hosts: 8009/tcp → 192.168.137.129

- Detect RPC over TCP: là một plugin giúp phát hiện dịch vụ Portmapper (còn gọi là RPC Portmapper) trên một máy mục tiêu. Dịch vụ này thường sử dụng cổng 111/tcp để ánh xạ các dịch vụ RPC với các cổng động. Khi một dịch vụ RPC được yêu cầu, Portmapper cung cấp thông tin về cổng động mà dịch vụ đó sẽ sử dụng

The screenshot shows the Tenable Nessus Essentials interface with the 'Vulnerabilities' tab selected. The main content area displays two findings:

Severity	Vulnerability Name	Family	Count
INFO	Nessus SYN scanner	Port scanners	25
INFO	Nessus Scan Information	Settings	1

Scan Details

- Policy: Advanced Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 4:53 PM
- End: Today at 4:56 PM
- Elapsed: 3 minutes

Vulnerabilities

A pie chart showing the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (blue).

The screenshot shows a web browser window with the URL <https://localhost:3834/#/scans/reports/9/vulnerabilities/19506>. The page displays 'Nessus Scan Information' for a scan of a Metasploitable 2 Linux host. The 'Description' section details the plugin's purpose and the information it provides about the scan. The 'Output' section shows the configuration and parameters used for the scan, including the Nessus version (10.8.3), build (20001), and feed version (202411161233). The 'Plugin Details' section includes metadata like Severity (Info), ID (19506), Version (1.127), Type (summary), Family (Settings), Published (August 26, 2005), and Modified (October 4, 2024). The 'Risk Information' section indicates a Risk Factor of None.