

BÁO CÁO THỰC HÀNH

Môn học: An toàn Mạng

Kỳ báo cáo: Buổi 02 (Session 02)

Tên chủ đề: Thu thập thông tin

GVHD: Nghi Hoàng Khoa

Ngày báo cáo: 18/10/2023

Nhóm: 08 (ghi số thứ tự nhóm)

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT140.O11.ANTN

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

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Câu 1, 2, 3, 4, 5, 6, 7, 23, 24, 30	100%

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

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

BÁO CÁO CHI TIẾT

Câu 1: Từ trang web của MegaCorp One, hãy mô tả một chút về lĩnh vực hoạt động của công ty?.

Trả lời:

- MegaCorp One chuyên hoạt động trong ngành công nghệ nano. Chịu trách nhiệm xác định các tiêu chuẩn của ngành trong lĩnh vực y tế, điện tử và thương mại.
- MegaCorp One cung cấp công nghệ từ máy bơm tim đến vũ khí thông minh, cho cả người tiêu dùng và cơ quan chính phủ.

MegaCorp One

About Us

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

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

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

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

Our team is creating the building blocks of modern society, where technology and life are inseparable.

We continue to strive for a better world by creating a society that is integrated into our framework.

History

MegaCorp One began as a computer processor start-up that grew tired of artificially limiting technology to extend profit margins.

We had technology in our engineering labs that exceeded anything available to the consumer, but we were limited by government contracts and investor expectations. This frustrated a group of us, and we decided to start our own company, that focused on providing bleeding edge technology directly to the consumer.

Our release of bleeding edge processors, that were substantially smaller and more efficient, lead to the creation of the term "nanotechnology." This buzzword further fueled our growth and allowed us to fund research in multiple industries.

We now offer technology that is found in everything ranging from heart pumps to smart weapons, with both consumer and government agencies as our customers.

Câu 2: 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)?

Trả lời:


Những thành viên đang làm việc cho MegaCorp One và một vài thông tin về những thành viên đó:

MegaCorp One[HOME](#)[ABOUT](#)[CONTACT](#)[SUPPORT](#)[CAREERS](#)[LOG IN](#)


MEET OUR TEAM




Joe Sheer
CHIEF EXECUTIVE OFFICER
Email: joe@megacorpone.com
Twitter: @Joe_Sheer



Tom Hudson
WEB DESIGNER
Email: thudson@megacorpone.com
Twitter: @TomHudsonMCO



Tanya Rivera
SENIOR DEVELOPER
Email: trivera@megacorpone.com
Twitter: @TanyaRiveraMCO



Matt Smith
MARKETING DIRECTOR
Email: msmith@megacorpone.com
Twitter: @MattSmithMCO

Câu 3: Khi có được địa chỉ Email của các thành viên thuộc tổ chức, bạn có phát hiện ra được điều gì?.

Trả lời:

- Email của các thành viên đang làm việc cho MegaCorp One đều có tên công ty làm domain (@megacorpone.com). Có thể suy ra được email của các nhân viên thuộc công ty này là <user>@megacorpone.com

Câu 4: Sử dụng công cụ whois để xác định các name server của MegaCorp One.

Trả lời:

Các name server là:

- NS1.MEGACORPONE.COM
- NS2.MEGACORPONE.COM
- NS3.MEGACORPONE.COM

```
(kali@kali)-[/home/kali]
PS> whois megacorpone.com
Domain Name: MEGACORPONE.COM
Registry Domain ID: 1775445745_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 2023-06-13T18:08:24Z
Creation Date: 2013-01-22T23:01:00Z
Registry Expiry Date: 2024-01-22T23:01:00Z
Registrar: Gandi SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse@support.gandi.net
Registrar Abuse Contact Phone: +33.170377661
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.MEGACORPONE.COM
Name Server: NS2.MEGACORPONE.COM
Name Server: NS3.MEGACORPONE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-10-18T02:08:05Z <<<
```

Ảnh lệnh và kết quả.

Câu 5: Sử dụng công cụ whois để tìm kiếm các thông tin của trường Đại học Công nghệ. Thông tin (uit.edu.vn) có được không? Giải thích?.

Trả lời:

```
(kali@kali)-[/home/kali]
PS> whois uit.edu.vn
This TLD has no whois server, but you can access the whois database at
http://www.vnnic.vn/en
```

Ảnh lệnh và kết quả.

- Không thể xem được vì TLD(Top-Level Domain) này không có whois server, tức là không thể tra cứu thông tin trực tiếp từ dịch vụ whois thông thường. Tuy nhiên, ta có thể truy cập cơ sở dữ liệu whois tại địa chỉ sau: <http://www.vnnic.vn/en>
- VNNIC (Việt Nam Network Information Center) là tổ chức quản lý tên miền quốc gia của Việt Nam và cung cấp dịch vụ whois cho các tên miền có đuôi ".vn" hoặc tên miền thuộc lãnh thổ quốc gia Việt Nam.

Câu 6: 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:

- Ta có thể truy cập cơ sở dữ liệu whois tại địa chỉ sau: <http://www.vnnic.vn/en>
- VNNIC (Việt Nam Network Information Center) là tổ chức quản lý tên miền quốc gia của Việt Nam và cung cấp dịch vụ whois cho các tên miền có đuôi ".vn" hoặc tên miền thuộc lãnh thổ quốc gia Việt Nam.
- Do đó ta có thể search:

VNNIC INTERNET RESOURCE WHOIS INFORMATION

This whois query was received from IP Address: **2a09:bac1:7ae0:10::246:3**
We recognize the resource in your query is: **Domain Name**
Type of domain name: **ASCII Domain Name**
Keyword in your query: **uit.edu.vn**

Domain information

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

Keyword *

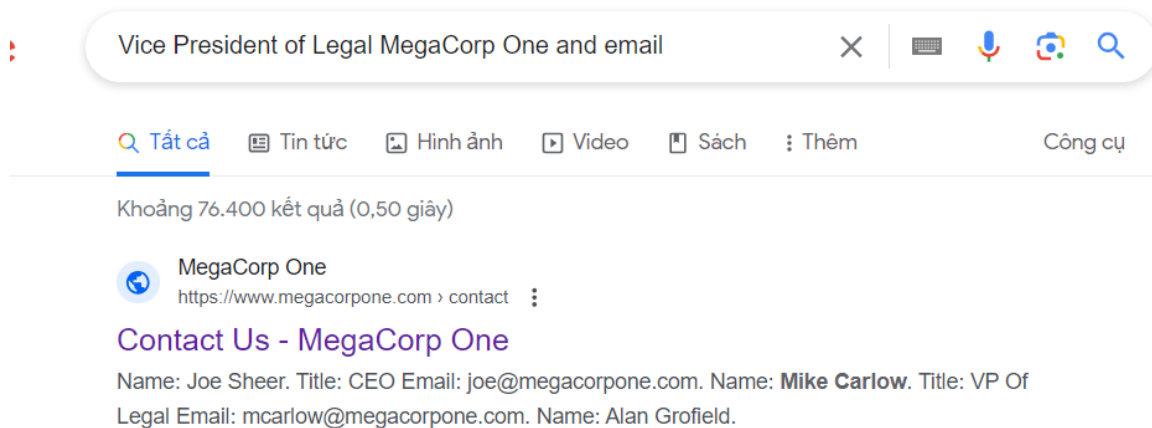
uit.edu.vn

- Ngày đăng ký tên miền : 2006-10-02
- Ngày hết hạn tên miền: 2024-10-02
- Chủ sở hữu tên miền: Công Ty TNHH PA VietNam
- Các name server của tên miền:
 - ns1.pavietnam.vn
 - ns2.pavietnam.vn
 - nsbak.pavietnam.net



Câu 7: Ai là Phó chủ tịch Pháp lý (Vice President of Legal) của MegaCorp One và địa chỉ email của họ là gì?

Trả lời: Ta search “Vice President of Legal MegaCorp One and email” → truy cập vào trang web như ảnh dưới đây.



Ảnh kết quả.

→ Kéo xuống cuối sẽ có thông tin cần tìm (tên và email của Vice President of Legal MegaCorp).

Email: joe@megacorpone.com
Name: Mike Carlow
Title: VP Of Legal
Email: mcarlow@megacorpone.com

Ảnh kết quả.

Câu 23: 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: Các địa chỉ IP đều giống nhau vì cấu hình DNS của tên miền uit.edu.vn có sử dụng wildcard * nên nếu xảy ra trường hợp 1 DNS query nào đó không có hostname thì sẽ được match với wildcard * trả về cùng 1 IP.


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

(kali@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

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

Ảnh lệnh và kết quả.

Câu 24: Sử dụng wordlist thông dụng khác (rockyou, seclists) để tìm kiếm các hostname hợp lệ khác của megacorpone.com

Trả lời: Sử dụng wordlist:

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

→ Dùng lệnh: `for hostname in $(cat list.txt); do host $hostname.megacorpone.com; done | grep -v "not found".`

```
(kali@kali)-[~]
$ for hostname in $(cat list.txt); do host $hostname.megacorpone.com; done
| grep -v "not found"
www.megacorpone.com has address 149.56.244.87
mail.megacorpone.com has address 51.222.169.212
ns1.megacorpone.com has address 51.79.37.18
ns2.megacorpone.com has address 51.222.39.63
test.megacorpone.com has address 51.222.169.219
www2.megacorpone.com has address 149.56.244.87
ns3.megacorpone.com has address 66.70.207.180
admin.megacorpone.com has address 51.222.169.208
mail2.megacorpone.com has address 51.222.169.213
vpn.megacorpone.com has address 51.222.169.220
beta.megacorpone.com has address 51.222.169.209
support.megacorpone.com has address 51.222.169.218
intranet.megacorpone.com has address 51.222.169.211
router.megacorpone.com has address 51.222.169.214
syslog.megacorpone.com has address 51.222.169.217
fs1.megacorpone.com has address 51.222.169.210

(kali@kali)-[~]
$
```

Ảnh lệnh và kết quả.

Câu 30: Thực hiện bắt Wireshark để mô tả cách gói tin được gửi và nhận khi thực hiện TCP Connect Scan sử dụng Nmap.

Trả lời:

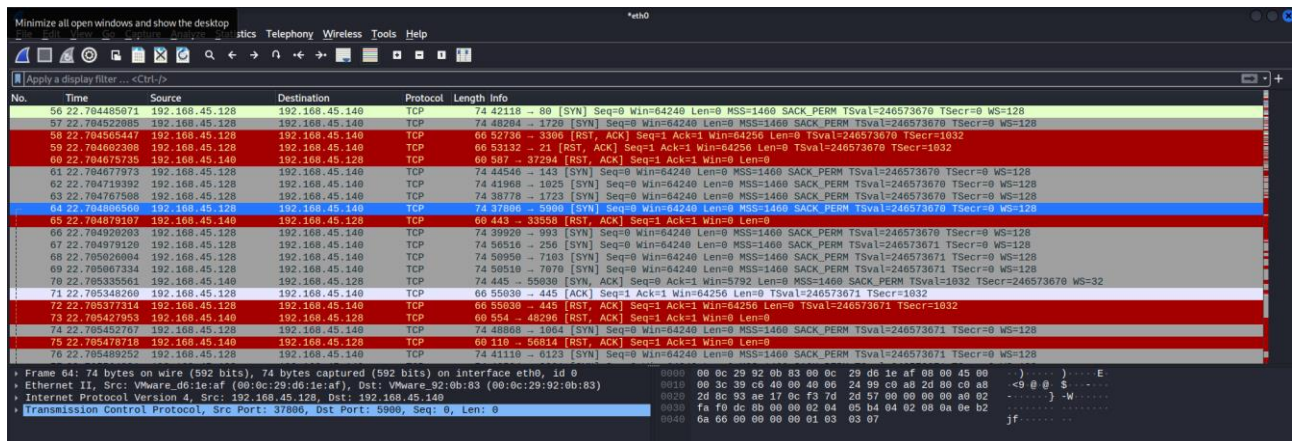
Dùng “nmap -sT” để thực hiện TCP connect scan. Ta quét máy Metasploitable 2 có địa chỉ 192.168.111.150.

```
(kali㉿kali)-[~]
$ nmap -sT 192.168.45.140
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-17 23:20 EDT
Nmap scan report for 192.168.45.140
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

Ảnh lệnh và kết quả.

Ta bắt lấy rất nhiều gói tin khi bắt bằng wireshark:



Ảnh bắt wireshark.

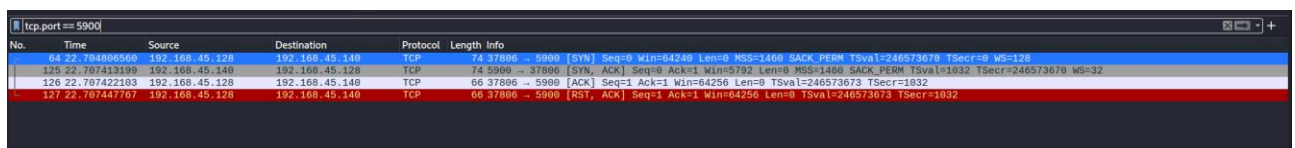
Từ kết quả sau khi chạy nmap, ta thử kiểm tra lại xem port 5900 có đang mở không:

Ở gói 64, máy ta gửi gói SYN tới 192.168.5.133.

Ở gói 125, máy 192.168.5.133 gửi gói SYN/ACK tới lại máy ta.

Ở gói 126 và 127, máy ta phản hồi lại gói ACK và gói RST, ACK cho máy 192.168.45.140

→ Kết luận: port 5900 đang mở.



Ảnh quá trình bắt tay ba bước.

YÊU CẦU CHUNG

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

Báo cáo:

- File **.DOCX và .PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).
Ví dụ: [NT101.K11.ATCL]-Session1_Group3.
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm bài Lab.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

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

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

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

HẾT