

BÁO CÁO THỰC HÀNH

Môn học: An toàn Mạng máy tính

Tên chủ đề: THU THẬP THÔNG TIN

GVHD: Tô Trọng Nghĩa

Nhóm: 18

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT140.O11.ANTT.1

| STT | Họ và tên | MSSV | Email |
|-----|---------------------|----------|------------------------|
| 1 | Nguyễn Lê Thảo Ngọc | 21521191 | 21521191@gm.uit.edu.vn |
| 2 | Trần Lê Minh Ngọc | 21521195 | 21521195@gm.uit.edu.vn |

2. NỘI DUNG THỰC HIỆN:¹

| STT | Nội dung | Tình trạng | Trang |
|------------------|---------------------------|------------|-------|
| 1 | Làm 35 câu bài tập về nhà | 100% | |
| Điểm tự đánh giá | | | 9/10 |

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

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

Lĩnh vực hoạt động: ngành công nghệ nano.

- 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)?

Địa chỉ email, chức vụ, tài khoản mạng xã hội của các thành viên được thể hiện ở ảnh sau:

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

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

Đuôi email là “megacorpone.com” => dễ nhận thấy họ là nhân viên của megacorpone

- Sử dụng công cụ whois để xác định các name server của MegaCorp One.

MegaCorp One có 3 name server: NS1.MEGACORPONE.COM, NS2.MEGACORPONE.COM, NS3.MEGACORPONE.COM

```
(bun㉿kali)-[~]
$ whois megacorpone.com
Domain Name: MEGACORPONE.COM
Registry Domain ID: 1775445745_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 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: 2023-10-25T13:29:26Z <<<
```

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?

```
This TLD has no whois server, but you can access the whois database at
http://www.vnnic.vn/en

(bun㉿kali)-[~]
```

Không dùng whois để tìm kiếm các thông tin của uit.edu.vn được vì whois server không hỗ trợ cho TLD .vn

1 số TLD mà whois cũng không hỗ trợ:

| TLD | Current response |
|-----|--|
| .al | This TLD has no whois server. |
| .cw | This TLD has no whois server. |
| .gr | This TLD has no whois server, but you can access the whois database at https://grweb.ics.forth.gr/public/whois |
| .mp | This TLD has no whois server. |
| .sr | This TLD has no whois server. |
| .to | Only nameservers |
| .vn | This TLD has no whois server, but you can access the whois database at http://www.vnnic.vn/en |

6. Thu thập thông tin về tên miền uit.edu.vn và hãy cho biết các thông tin như sau:

This whois query was received from IP Address: 113.185.73.136
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 *

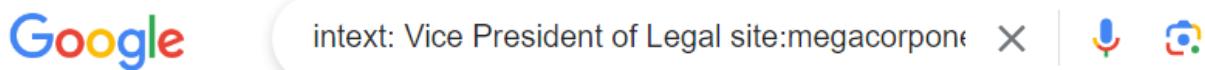
CAPTCHA

Từ thông tin tìm được từ www.vnnic.vn/en

- a. Ngày đăng ký tên miền: 2/10/2006
 - b. Ngày hết hạn tên miền: 2/10/2024
 - c. Chủ sở hữu tên miền: Công ty TNHH PA Việt Nam
 - d. Các name server của tên miền:
ns1.pavietnam.vn;
ns2.pavietnam.vn;
nsbak.pavietnam.net
7. 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: Mike Carlow

Địa chỉ email: mcarlow@megacorpone.com



All

News

Images

Videos

Books

More

About 1 results (0.23 seconds)



megacorpone.com

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

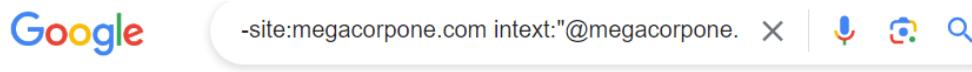
⋮

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.

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

Dùng thêm cú pháp: -site:megacorpone.com để không tìm kiếm ở các trang web www.megacorpone.com



All

Videos

News

Shopping

Images

More

Tools

About 16,800 results (0.28 seconds)



linkedin.com

<https://www.linkedin.com> › company › megacorp-one

⋮

MegaCorp One

<http://www.megacorpone.com>. External link for MegaCorp One. Industry: Nanotechnology Research. Company size: 501-1,000 employees. Headquarters: Rachel, NV. Type ...



github.com

<https://github.com> › megacorpone

⋮

MegaCorp One megacorpone

2 Old Mill St Rachel, NV 89001; <http://www.megacorpone.com> · Achievements ... Popular repositories. megacorpone.com Public. dev backup for main site. CSS 27 47.



github.com

<https://github.com> › blob › master › megacorpone › a...

⋮

about.html

... megacorpone.com">SUPPORT JOBS LOG IN </div><!--.nav ...



twitter.com

<https://twitter.com> › RealWillAdler

⋮

RealWillAdler - William Adler

I'm not sure yet.. Nevada, USA megacorpone.com Born 1985 Joined September 2017. 7

9. Liệt kê một vài từ khóa thường gặp trên Google và cho ví dụ? (Yêu cầu: ít nhất 5 từ khóa)
- intitle:"tin tức"

Google search results for "intitle:'tin tức'"

About 10,900,000 results (0.46 seconds)

Báo Thanh Niên
https://thanhnien.vn

Báo Thanh Niên: Tin tức 24h mới nhất, tin nhanh, tin nóng ...
Tin tức 24h, đọc báo TN cập nhật tin nóng online Việt Nam và thế giới mới nhất trong ngày, tin nhanh thời sự, chính trị, xã hội hôm nay, tin tức, top news ...
Tin tức, thời sự quốc tế, an... · Tin tức Công nghệ · Video · Tin 24h

Báo Dân trí
https://dantri.com.vn

Báo Dân trí: Tin tức Việt Nam và quốc tế nóng, nhanh, cập ...
Đọc báo dantri - Tin tức mới nhất, Thông tin nhanh chính xác được cập nhật hàng giờ. báo nói đọc tin tức online Việt Nam Thế giới nóng nhất trong ngày, ...

Videos

- inurl:"password"

About 33,900,000 results (0.31 seconds)

Wikipedia
https://en.wikipedia.org › wiki › Password

Password
A password, sometimes called a passcode is secret data, typically a string of characters, usually used to confirm a user's identity.

Cambridge Dictionary
https://dictionary.cambridge.org › dictionary › password

PASSWORD | English meaning - Cambridge Dictionary
a secret word or combination of letters or numbers, used for communicating with another person or with a computer to prove who you are:

LastPass
https://www.lastpass.com › features › password-genera...

Password Generator
Need a Unique, Secure Password? Generate, save, and autofill credentials across all your devices with LastPass. Start Free LastPass Trial.

- “movie”

Google "movie" X |  

All Videos Images News More

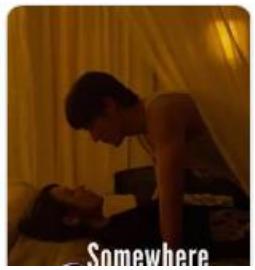
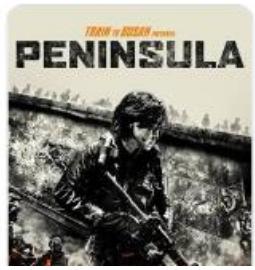
About 3,770,000,000 results (0.65 seconds)

What to watch  Recommended for you [Learn more](#)

Movies ▾ New Drama Netflix Action Comedy Horror Romance

Top picks for you



- “Music”

Google "music" X |  

All Videos Images Books Shopping More Tool

About 5,000,000,000 results (0.37 seconds)

 YouTube Music
<https://music.youtube.com> :

[YouTube Music](#)
A new **music** service with official albums, singles, videos, remixes, live performances and more for Android, iOS and desktop. It's all here.

 Videos :

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

VD1:Tìm kiếm với từ: password

Sử dụng từ khoá: iurl:"uit.edu.vn" -> để giới hạn chỉ tìm kiếm các tài liệu của Trường Đại học Công nghệ Thông tin mà được công bố trên Internet

- Kết quả:

Google search results for "password iurl:'uit.edu.vn'"

- Trường Đại học Công nghệ Thông tin**
https://phongdl.uit.edu.vn › gmail-c...
Hướng dẫn sử dụng mail.gm.uit.edu.vn cho sinh viên.
Aug 20, 2012 — 1/ Hướng dẫn kích hoạt tài khoản. Mở trình duyệt web. Nhập mail.gm.uit.edu.vn, màn hình xuất hiện như sau. Nhập Username và Password đã được ...
- Trường Đại học Công nghệ Thông tin**
https://www.uit.edu.vn › huong-dan...
Hướng dẫn sử dụng tài khoản chứng thực và ...
Mar 21, 2022 — Tài khoản email sinh viên: http://mail.gm.uit.edu.vn (username: *****@gm.uit.edu.vn, password: *****). Tài khoản Office365 để đăng nhập ...
- Trường Đại học Công nghệ Thông tin**
https://ctsv.uit.edu.vn › bai-viet › fo...
Forum đã hoạt động trở lại và thông báo về tài khoản SV trên ...
Oct 2, 2019 — ... password và lấy lại password mới qua email gm.uit.edu.vn. - Nếu có ...
Website Đoàn - Hội · Website ĐH Quốc gia · Website ký túc xá. Kết nối với ...

Thông báo về việc sử dụng kho tài liệu số của ĐHQG-HCM ...
Apr 22, 2023 — Link thư viện UIT : http://thuvien.uit.edu.vn/. Sinh viên đăng nhập ... (User và Pass: như trên). Link giới thiệu App: https://www.youtube.com ...

- Truy cập vô 1 trang web bên dưới(chỗ khoanh tròn):



CITD - Thông báo về việc sử dụng kho tài liệu số của ĐHQG-HCM và UIT đối với các sinh viên khóa K2022.3

17, 22/04/2023 - 12:59

Chào các anh chị Sinh viên khóa K2022.3! Để phục vụ việc học tập tốt và hiệu quả hơn.

PDT CITD xin giới thiệu đến các anh, chị kho tài nguyên – tài liệu số của UIT:

- Link thư viện UIT : <http://thuvien.uit.edu.vn/>

Sinh viên đăng nhập với tài khoản chứng thực

Thư viện ĐHQG : <https://opac.vnulib.edu.vn/>

Sinh viên đăng nhập với tài khoản:

ID: 15000+MSSV

password: 1...8

Sau khi đăng nhập nên đổi password

Với Mã thẻ thư viện và Password này, Sinh viên đăng nhập để:

Tra cứu OPAC (Công tra cứu nguồn tài liệu chung của Hệ thống Thư viện ĐHQG-HCM, bản in):
<https://opac.vnulib.edu.vn/>

- MSSV là thông tin rất dễ biết nên nếu sinh viên chưa kịp đổi tài khoản mặc định thì sẽ dễ bị mất tài khoản hoặc bị kẻ xấu lợi dụng tài khoản.

VD2: Tìm kiếm với từ: danh sach

Sử dụng từ khoá: iurl:"uit.edu.vn" -> để giới hạn chỉ tìm kiếm các tài liệu của Trường Đại học Công nghệ Thông tin mà được công bố trên Internet

- Kết quả: có khoảng 191000 kết quả trong 0.22s

Google

danh sach iurl:uit.edu.vn

Trường Đại học Công nghệ Thông tin
<https://ctsv.uit.edu.vn/bai-viet/ca...>

Cập nhật dữ liệu sinh viên | Phòng Công tác Sinh viên

Apr 18, 2023 — Danh sách sinh viên thiếu hồ sơ nhập học - Khóa 2023 ... Ngày cấp, nơi cấp CCCD;. Sinh viên cập nhật qua form <https://link.uit.edu.vn/CapNhat-CCCD>.

Trường Đại học Công nghệ Thông tin
<https://www.uit.edu.vn/danh-sach...>

Danh sách sinh viên tham gia training Kỹ năng thông tin

Mar 11, 2023 — Thư viện UIT gửi các bạn danh sách đăng ký tham gia vào các buổi: ... - Thư viện vẫn còn tiếp nhận đăng ký qua link: <https://link.uit.edu.vn/> ...

Trường Đại học Công nghệ Thông tin
<https://ctsv.uit.edu.vn>

ctsv@uit.edu.vn

Thông báo danh sách đăng ký Học bổng KKHT HK2 2022-2023 và Học bổng Ngoài ... Website liên kết. Website Trường · Forum Trường · Website Đoàn - Hội · Website ĐH ...

Trường Đại học Công nghệ Thông tin
<https://ctsv.uit.edu.vn/node>

Danh sách sinh viên cập nhật BHYT | Phòng Công tác Sinh viên

Aug 3, 2023 — ... danh sách cập nhật, Phòng Công tác Sinh viên đã công bố vào ngày 28/7/2023, link <https://ctsv.uit.edu.vn/bai-viet/danh-sach-sv-cap-nhat-bhyt...>

- Truy cập vô 1 trang web bên dưới(chỗ khoanh tròn):

Danh sách sinh viên cập nhật BHYT

Thu, 03/08/2023 - 10:36

Phòng Công tác Sinh viên thông báo danh sách cập nhật BHYT phi
tác chấm điểm rèn luyện HK2 năm học 2022-2023 như sau:

Sau khi rà soát danh sách cập nhật, Phòng Công tác Sinh viên đã c
ngày 28/7/2023, link <https://ctsv.uit.edu.vn/bai-viet/danh-sach-sv-cap-bhyt-hk2-nam-hoc-...> và phản hồi của sinh viên ở
forum <https://forum.uit.edu.vn/node/564756#post565061>

Có nhiều trường hợp sinh viên đã được cộng điểm rèn luyện HK2 n
nhưng vẫn cập nhật BHYT. Qua kiểm tra đối chiếu, Phòng Công tác
bỏ những sinh viên cập nhật dư/thừa và chỉ còn lại 77 sinh viên theo
sách đính kèm.

| STT | | HỌ TÊN | HSD THẺ |
|-----|----------|---------------------|------------|
| 1 | 17520057 | Đoàn Thanh Hiền | 2024-06-30 |
| 2 | 17520476 | Lê Trung Hiếu | 2023-12-31 |
| 3 | 17520979 | Trương Hữu Sang | 2023-12-31 |
| 4 | 17521072 | Lê Hoàng Phương Thê | 2023-06-30 |
| 5 | 18520293 | Trần Cao Việt Khoa | 2023-06-30 |
| 6 | 18520584 | Phạm Quốc Đạt | 2023-12-31 |
| 7 | 18520656 | Đặng Ngọc Khánh Duy | 2023-12-31 |
| 8 | 18520708 | Trần Trung Hải | 2023-12-31 |

=> biết được MSSV của rất nhiều sinh viên

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

Từ kết quả trả về sau khi dùng Netcraft để tìm thông tin về www.megacorpone.com

Ta thấy application server của megacorpone: ns1.megacorpone.com

Nhóm 18

| | |
|-------------------------|--|
| IPv4 address | 149.56.244.87 (VirusTotal) |
| IPv4 autonomous systems | AS16276 [?] |
| IPv6 address | Not Present |
| IPv6 autonomous systems | Not Present |
| Reverse DNS | www.megacorpone.com |
| Domain | megacorpone.com |
| Nameserver | ns1.megacorpone.com |
| Domain registrar | gandi.net |
| Nameserver organisation | whois.gandi.net |
| Organisation | MegaCorpOne, Rachel, 89001, United States |
| DNS admin | admin@megacorpone.com |
| Top Level Domain | Commercial entities (.com) |

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

- Tìm kiếm địa chỉ IP của các host có tên miền medacorpone bằng module: brute_hosts

```
[recon-ng][default] > modules load recon/domains-hosts/brute_hosts
[recon-ng][default][brute_hosts] > run

MEGACORPONE.COM

[*] No Wildcard DNS entry found.
[*] 03.megacorpone.com => No record found.
[*] 0.megacorpone.com => No record found.
[*] 01.megacorpone.com => No record found.
[*] 1.megacorpone.com => No record found.
[*] 11.megacorpone.com => No record found.
[*] 02.megacorpone.com => No record found.
[*] 14.megacorpone.com => No record found.
[*] 10.megacorpone.com => No record found.
[*] 13.megacorpone.com => No record found.
```

- Hiển thị thông tin của các host đã tìm được ứng với tên miền medacorpone bằng lệnh: show hosts

```
[recon-ng][default][brute_hosts] > show hosts
+-----+
| rowid | updatetime | host | ip_address | region | country | latitude | longitude | notes | module |
+-----+
| 1 | 2023-09-12T10:24:54Z | www.megacorpone.com | 149.56.244.87 | North America | United States | 37.7749 | -122.4194 | | google_site_web |
| 241 | 2023-09-12T10:24:54Z | admin.megacorpone.com | 149.56.244.87 | North America | United States | 37.7749 | -122.4194 | | brute_hosts |
| 3 | 2023-09-12T10:24:54Z | beta.megacorpone.com | 149.56.244.87 | North America | United States | 37.7749 | -122.4194 | | brute_hosts |
| 4 | 2023-09-12T10:24:54Z | intranet.megacorpone.com | 149.56.244.87 | North America | United States | 37.7749 | -122.4194 | | brute_hosts |
| 5 | 2023-09-12T10:24:54Z | mail2.megacorpone.com | 149.56.244.87 | North America | United States | 37.7749 | -122.4194 | | brute_hosts |
| 6 | 2023-09-12T10:24:54Z | mail.megacorpone.com | 149.56.244.87 | North America | United States | 37.7749 | -122.4194 | | brute_hosts |
| 7 | 2023-09-12T10:24:54Z | ns2.megacorpone.com | 149.56.244.87 | North America | United States | 37.7749 | -122.4194 | | brute_hosts |
| 8 | 2023-09-12T10:24:54Z | ns1.megacorpone.com | 149.56.244.87 | North America | United States | 37.7749 | -122.4194 | | brute_hosts |
| 9 | 2023-09-12T10:24:54Z | ns3.megacorpone.com | 149.56.244.87 | North America | United States | 37.7749 | -122.4194 | | brute_hosts |
| 10 | 2023-09-12T10:24:54Z | router.megacorpone.com | 149.56.244.87 | North America | United States | 37.7749 | -122.4194 | | brute_hosts |
| 11 | 2023-09-12T10:24:54Z | smmp.megacorpone.com | 149.56.244.87 | North America | United States | 37.7749 | -122.4194 | | brute_hosts |
| 12 | 2023-09-12T10:24:54Z | support.megacorpone.com | 149.56.244.87 | North America | United States | 37.7749 | -122.4194 | | brute_hosts |
| 13 | 2023-09-12T10:24:54Z | syslog.megacorpone.com | 149.56.244.87 | North America | United States | 37.7749 | -122.4194 | | brute_hosts |
| 14 | 2023-09-12T10:24:54Z | test.megacorpone.com | 149.56.244.87 | North America | United States | 37.7749 | -122.4194 | | brute_hosts |
| 15 | 2023-09-12T10:24:54Z | vpn.megacorpone.com | 149.56.244.87 | North America | United States | 37.7749 | -122.4194 | | brute_hosts |
| 16 | 2023-09-12T10:24:54Z | www.megacorpone.com | 149.56.244.87 | North America | United States | 37.7749 | -122.4194 | | brute_hosts |
| 17 | 2023-09-12T10:24:54Z | www2.megacorpone.com | 149.56.244.87 | North America | United States | 37.7749 | -122.4194 | | brute_hosts |

+-----+
[*] 17 rows returned
```

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

1.Tìm địa chỉ IP ứng với miền: uit.edu.vn

- Tìm kiếm địa chỉ IP của các host có tên miền uit.edu.vn bằng module: brute_hosts

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

UIT.EDU.VN
_____
[*] Wildcard DNS entry found for 'uit.edu.vn' at '45.122.249.78'.
[*] 02.uit.edu.vn => (A) 118.69.123.140
[*] 03.uit.edu.vn => Response matches the wildcard.
[*] 0.uit.edu.vn => (A) 118.69.123.140
[*] 10.uit.edu.vn => (A) 118.69.123.140
[*] 01.uit.edu.vn => Response matches the wildcard.
[*] 14.uit.edu.vn => (A) 118.69.123.140
[*] 13.uit.edu.vn => (A) 118.69.123.140
[*] 1.uit.edu.vn => Response matches the wildcard.
[*] 11.uit.edu.vn => Response matches the wildcard.
[*] 12.uit.edu.vn => (A) 118.69.123.140
[*] Country: None
[*] Host: 02.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Country: None
[*] Host: 0.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Notes: None
[*] Country: None
[*] Host: 10.uit.edu.vn
```

| Rank | Site |
|---------|-------------------|
| 45824 | www.megacorp |
| 749770 | support.megacorp |
| 991741 | intranet.megacorp |
| 1410584 | admin.megacorp |

- Hiển thị thông tin của các host đã tìm được ứng với tên miền medacorpone bằng lệnh: show host

| rowid | host | ip_address | region | country | latitude | longitude | notes | module |
|-------|-----------------|----------------|--------|---------|----------|-----------|-------|-------------|
| 19 | 0.uit.edu.vn | 118.69.123.140 | | | | | | brute_hosts |
| 20 | 10.uit.edu.vn | 118.69.123.140 | | | | | | brute_hosts |
| 21 | 13.uit.edu.vn | 118.69.123.140 | | | | | | brute_hosts |
| 22 | 02.uit.edu.vn | 45.122.249.78 | | | | | | brute_hosts |
| 23 | 0.uit.edu.vn | 45.122.249.78 | | | | | | brute_hosts |
| 24 | 12.uit.edu.vn | 118.69.123.140 | | | | | | brute_hosts |
| 25 | 12.uit.edu.vn | 45.122.249.78 | | | | | | brute_hosts |
| 26 | 13.uit.edu.vn | 45.122.249.78 | | | | | | brute_hosts |
| 27 | 15.uit.edu.vn | 118.69.123.140 | | | | | | brute_hosts |
| 28 | 10.uit.edu.vn | 45.122.249.78 | | | | | | brute_hosts |
| 29 | 14.uit.edu.vn | 118.69.123.140 | | | | | | brute_hosts |
| 30 | 18.uit.edu.vn | 118.69.123.140 | | | | | | brute_hosts |
| 31 | 18.uit.edu.vn | 45.122.249.78 | | | | | | brute_hosts |
| 32 | 14.uit.edu.vn | 45.122.249.78 | | | | | | brute_hosts |
| 33 | 19.uit.edu.vn | 118.69.123.140 | | | | | | brute_hosts |
| 34 | 19.uit.edu.vn | 45.122.249.78 | | | | | | brute_hosts |
| 35 | 20.uit.edu.vn | 118.69.123.140 | | | | | | brute_hosts |
| 36 | 2.uit.edu.vn | 118.69.123.140 | | | | | | brute_hosts |
| 37 | 2.uit.edu.vn | 45.122.249.78 | | | | | | brute_hosts |
| 38 | 20.uit.edu.vn | 45.122.249.78 | | | | | | brute_hosts |
| 39 | 4.uit.edu.vn | 118.69.123.140 | | | | | | brute_hosts |
| 40 | 3com.uit.edu.vn | 118.69.123.140 | | | | | | brute_hosts |
| 41 | 3.uit.edu.vn | 118.69.123.140 | | | | | | brute_hosts |

=> miền uit.edu.vn chỉ có 2 IP address: 118.69.123.140, 45.122.249.78

2. Tìm các website có miền liên quan đến uit.edu.vn

- Dùng module: recon/domains-hosts/google_site_web

Nhóm 18

```
[recon-ng][default] > modules load recon/domains-hosts/google_site_web
[recon-ng][default][google_site_web] > options set SOURCE uit.edu.vn
SOURCE => uit.edu.vn
[recon-ng][default][google_site_web] > run

_____
UIT.EDU.VN
_____
[*] Searching Google for: site:uit.edu.vn
[*] Country: None
[*] Host: dsc.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: dsc.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
```

- Hiển thị thông tin của các host đã tìm được ứng với tên miền medacorpone bằng lệnh: show hosts

| File | Actions | Edit | View | Help |
|---------------------------------------|---------|---------------|------|-----------------|
| 1955 zw.uit.edu.vn | | 45.122.249.78 | | |
| 1956 dsc.uit.edu.vn | | | | brute_hosts |
| 1957 student.uit.edu.vn | | | | google_site_web |
| 1958 fce.uit.edu.vn | | | | google_site_web |
| 1959 khoaocitre.uit.edu.vn | | | | google_site_web |
| 1960 en.uit.edu.vn | | | | google_site_web |
| 1961 oep.uit.edu.vn | | | | google_site_web |
| 1962 thuvien.uit.edu.vn | | | | google_site_web |
| 1963 tuyensinh.uit.edu.vn | | | | google_site_web |
| 1964 inseclab.uit.edu.vn | | | | google_site_web |
| 1965 cnsc.uit.edu.vn | | | | google_site_web |
| 1966 ctsv.uit.edu.vn | | | | google_site_web |
| 1967 mapr.uit.edu.vn | | | | google_site_web |
| 1968 jobs.uit.edu.vn | | | | google_site_web |
| 1969 thilaptrinh.uit.edu.vn | | | | google_site_web |
| 1970 auth.uit.edu.vn | | | | google_site_web |
| 1971 survey.uit.edu.vn | | | | google_site_web |
| 1972 qhdn.uit.edu.vn | | | | google_site_web |
| 1973 dbcl.uit.edu.vn | | | | google_site_web |
| 1974 sdh.uit.edu.vn | | | | google_site_web |
| 1975 mitaka.uit.edu.vn | | | | google_site_web |
| 1976 vlab.uit.edu.vn | | | | google_site_web |
| 1977 daa.uit.edu.vn | | | | google_site_web |
| 1978 drl.uit.edu.vn | | | | google_site_web |
| 1979 congdoan.uit.edu.vn | | | | google_site_web |
| 1980 phongdl.uit.edu.vn | | | | google_site_web |
| 1981 khcn.uit.edu.vn | | | | google_site_web |
| 1982 banqlcs.uit.edu.vn | | | | google_site_web |
| 1983 kmkt.uit.edu.vn | | | | google_site_web |
| 1984 chungthuc.uit.edu.vn | | | | google_site_web |
| 1985 courses.uit.edu.vn | | | | google_site_web |
| 1986 danguy.uit.edu.vn | | | | google_site_web |
| 1987 qtib.uit.edu.vn | | | | google_site_web |
| 1988 khtc.uit.edu.vn | | | | google_site_web |
| 1989 tutorials.aiclub.cs.uit.edu.vn | | | | google_site_web |
| 1990 oms.uit.edu.vn | | | | google_site_web |
| 1991 mmlab.uit.edu.vn | | | | google_site_web |
| 1992 ctgt.uit.edu.vn | | | | google_site_web |
| 1993 fit.uit.edu.vn | | | | google_site_web |
| 1994 ptmhtt.uit.edu.vn | | | | google_site_web |
| 1995 tchc.uit.edu.vn | | | | google_site_web |
| 1996 nlp.uit.edu.vn | | | | google_site_web |
| 1997 portal.uit.edu.vn | | | | google_site_web |

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

- Dùng Gitleaks để phát hiện các secret trong repo Github

VD: Repository: TP-O/edusoft

Chức năng: Support register for courses and crawl your data on the HCMIU Edusoft website.

Phát hiện: 23 rủi ro trong source code

on Aug 6, 2021
+ 2 releases

Contributors 2
TP-O Tran Ph
dependabot

Languages
TypeScript 98.9%

README.md

[DEPRECATED], use <https://github.com/TP-O/goer> instead

EduSoft

EduSoft Package can help you get information from <https://edusoftweb.hcmiu.edu.vn> easily.

Installation

NPM

```
npm install edusoft
```

Yarn

```
yarn add edusoft
```

Usage

You need to provide credentials before using any feature that requires authentication.

```
const edu = require("edusoft");

edu.config({
    username: "<Student ID>",
    password: "<Password>",
});
```

News

Crawl all the news from <https://edusoftweb.hcmiu.edu.vn/default.aspx?page=dansachthongtin&type=0>.

```
(bun㉿kali)-[~/Downloads/Gitleaks/gitleaks]
$ gitleaks detect https://github.com/TP-O/edusoft.git -v

o
o documents
o
o gitleaks

Finding: Raw: `const Discord_Public_Key = "e7322523fb86ed64c836a979cf8465fdb436378c653c1db38f9ae87bc62a6fd5";`  

Secret: e7322523fb86ed64c836a979cf8465fdb436378c653c1db38f9ae87bc62a6fd5  

RuleID: discord-api-token  

Entropy: 3.790624  

File: detect/detect_test.go  

Line: 326  

Commit: 025908808f2ad1ce244f9806b8dd593bd9afbab0  

Author: raffis  

Email: raffael.sahlia@doodle.com  

Date: 2023-02-25T14:36:23Z  

Fingerprint: 025908808f2ad1ce244f9806b8dd593bd9afbab0:detect/detect_test.go:discord-api-token:326

Finding: -----BEGIN PRIVATE KEY BLOCK-----  

anything  

-----END PRIVATE KEY BLOCK-----  

Secret: -----BEGIN PRIVATE KEY BLOCK-----  

anything  

-----END PRIVATE KEY BLOCK-----  

RuleID: private-key  

Entropy: 4.090647  

File: cmd/generate/config/rules/privatekey.go  

Line: 26  

Commit: e002920355ac91770a329cfa69d6359bd665ba66  

Author: very-doge-wow  

Email: 95224950+very-doge-wow@users.noreply.github.com  

Date: 2023-01-12T14:38:48Z
```

Nhóm 18

```
Finding: Match: "pypi-AgEIcHlwaS5vcmcAAAAAAAAA-AAAAAAA-AAAAAAA-AAAAAAA-AAAAAAA-AAAAAAAAB",
Secret: pypi-AgEIcHlwaS5vcmcAAAAAAAAA-AAAAAAA-AAAAAAA-AAAAAAA-AAAAAAA-AAAAAAAAB
RuleID: pypi-upload-token
Entropy: 1.960688
File: detect/detect_test.go
Line: 33
Commit: 9326f35380636bcbe61e94b0584d1618c4b5c2c2
Author: Isaac Dawson
Email: 60455448+idawson-gl@users.noreply.github.com
Date: 2022-03-07T14:33:06Z
Fingerprint: 9326f35380636bcbe61e94b0584d1618c4b5c2c2:detect/detect_test.go:pypi-upload-token:33

7:55PM INF 811 commits scanned.
7:55PM INF scan completed in 1.12s
7:55PM WRN leaks found: 23
```

15. Thực hiện tìm kiếm các lệnh khác trên Shodan mà có thể tiết lộ thêm nhiều thông tin thú vị về một đối tượng bất kỳ.

- Tìm thông tin về host 45.122.249.78

| General Information | | Open Ports | |
|---------------------|---------------------------------|------------|-----|
| Hostnames | citd.vn static.cmcti.vn | 80 | 443 |
| Domains | CITD.VN CMCTI.VN | | |
| Country | Viet Nam | | |
| City | Ho Chi Minh City | | |
| Organization | Binh Duong Branch - CMC Telecom | | |

LAST SEEN: 2023-10-17

// 80 / TCP - 221918750 | 2023-10-07T19:38:24,349/785

HTTP/1.1 302 Found
content-length: 0
location: https://www.uitt.edu.vn
cache-control: no-cache

// 443 / TCP - 221918750 | 2023-10-09T11:01:14,846/988

- Tìm thông tin về port:

| Host | Location | Last Seen |
|----------------|---|-----------------------------|
| 82.151.125.26 | OJSC Rostelecom, Belgorod branch Russia, Valuyki | 2023-10-11T19:52:21,068/606 |
| 182.200.187.69 | CHINANET Liaoning province network China, Shenyang | 2023-09-29T23:22:11,635/520 |

- Tìm các thiết bị ở thành phố Hồ Chí Minh không dùng hệ điều hành Windows

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

- Tìm kiếm với từ khoá “host 45.122.249.78” bằng Google:

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

- Tìm kiếm với nguồn: bing

- Tìm kiếm với nguồn: bing

=> Tìm được 2 địa chỉ email liên quan uit:

+info@uit.edu.vn

+phongdaotaodh@uit.edu.vn

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

- Tìm kiếm với nguồn hackertarget

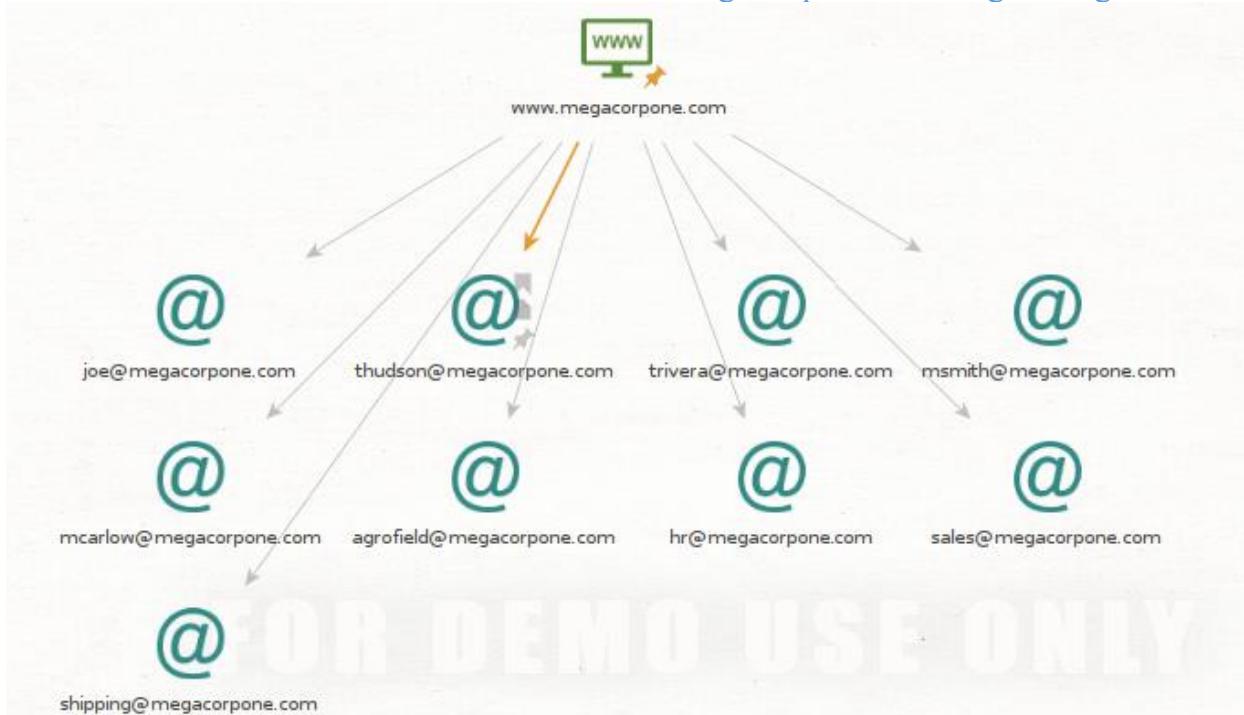
=> Không tìm được email nào

- Tìm kiếm với nguồn netlas

=> không tìm được thông tin gì liên quan đến miền uit.edu.vn

Trong các nguồn đã tìm kiếm thì bing dùng tốt hơn vì trả về nhiều kết quả hơn

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



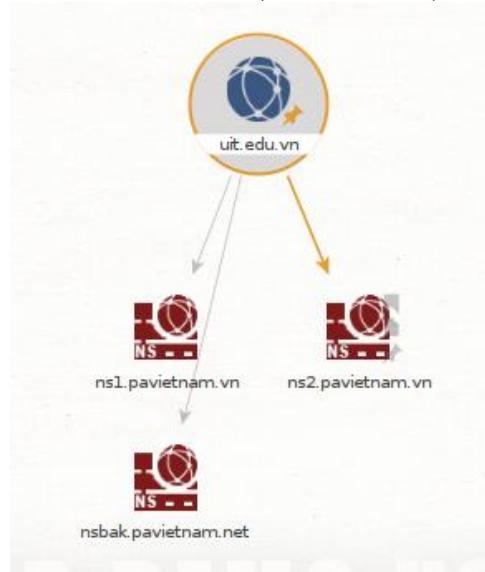
20. Sử dụng công cụ Maltego cho UIT (tên miền: uit.edu.vn) và trả lời các câu hỏi sau:

a. Các bản ghi DNS.

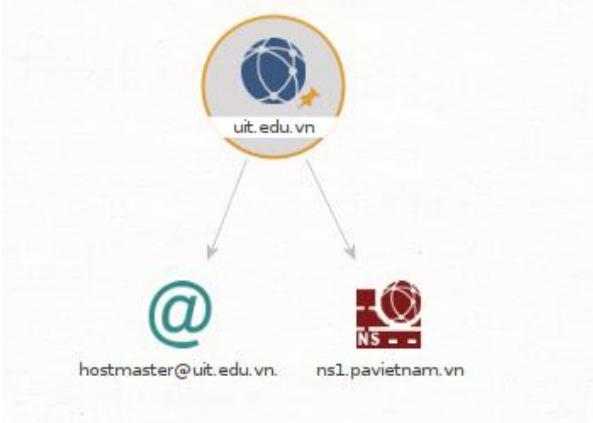
- Bản ghi MX: chọn To DNS Name - MX (mail server)



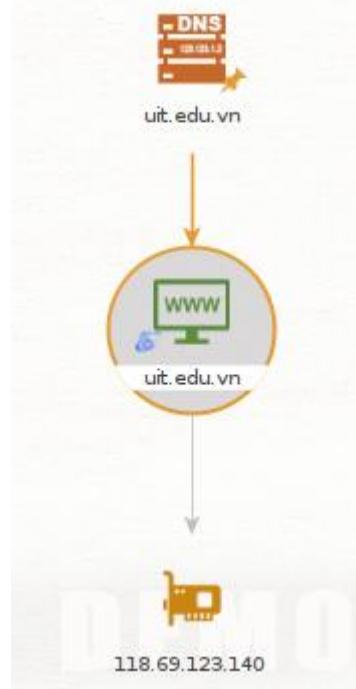
- Bản ghi NS: chọn To DNS Name - NS (name server)



- Bản ghi SOA: chọn To DNS Name - SOA (Start of Authority)



b. Các website và địa chỉ IP tương ứng.



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

- Bản ghi SOA (Start of Authority): bản ghi SOA chứa thông tin về tên miền cụ thể và xác định máy chủ chịu trách nhiệm quản lý tên miền đó.
- Bản ghi SRV (Service): là một loại bản ghi được sử dụng để xác định các dịch vụ và máy chủ cung cấp các dịch vụ đó trên mạng. Bản ghi SRV chứa thông tin về tên miền, cổng kết nối, giao thức, và độ ưu tiên của máy chủ cung cấp dịch vụ.
- Bản ghi SPF (Sender Policy Framework): là một loại bản ghi được sử dụng để xác định máy chủ email được phép gửi email thay mặt cho tên miền cụ thể. Bản ghi SPF chứa thông tin về máy chủ (hoặc địa chỉ IP) được phép gửi email từ tên miền đó.
- Bản ghi DKIM (DomainKeys Identified Mail): là bản ghi được sử dụng để xác minh tính xác thực của email và ngăn chặn gửi email giả mạo bằng cách đảm bảo rằng chỉ các máy chủ email được ủy quyền có khóa riêng hợp lệ mới có thể tạo chữ ký số DKIM cho tên miền đó.

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

- Bản ghi TXT:

```
(ngoc@ngoc)-[~]
$ host -t txt uit.edu.vn
uit.edu.vn descriptive text "svp60rjlwr6s19rn9t013cfwm3xmqx7h"
uit.edu.vn descriptive text "v=spf1 include:_spf.google.com ~all"
uit.edu.vn descriptive text "sqm6y27vn74pm290pl0fq4hcr08gst5r"
uit.edu.vn descriptive text "MS=E431E3CA3EFF5A6431E2378C924984A8A0334ABC"
uit.edu.vn descriptive text "google-site-verification=wjArKGa37oHK083XqT2C9
1tPny8NLttGS0aU5pJjKiY"
```

- Bản ghi MX:

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

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?

```
(ngoc@ngoc)-[~]
$ host www.uit.edu.vn
www.uit.edu.vn has address 118.69.123.140

(ngoc@ngoc)-[~]
$ 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

(ngoc@ngoc)-[~]
$ host noexist.uit.edu.vn
noexist.uit.edu.vn has address 118.69.123.140
noexist.uit.edu.vn has address 45.122.249.78

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

=> Kết quả không hiển thị lỗi mà hiển thị IP của trang web chính thức www.uit.edu.vn
Giải thích:

- Thay vì hiển thị các hostname không tồn tại như “idontexist.uit.edu.vn” hoặc “noexitst.uit.edu.vn”, trang web đã tự động chuyển hướng đến trang mặc định hoặc trang chính của tên miền “uit.edu.vn”. Điều này thường xảy ra khi máy chủ web của tên miền không tìm thấy hostname mà chúng ta cố gắng truy cập.
- Cơ chế chuyển hướng này có thể được cấu hình trên máy chủ web của tên miền “uit.edu.vn” để đảm bảo rằng người dùng không nhận được lỗi "Không thể tìm thấy trang" khi truy cập các hostname không tồn tại.
- Chuyển hướng này thường được thực hiện bằng cách sử dụng bản ghi DNS kiểu “wildcard” (dấu sao '*' trong bản ghi A hoặc CNAME) để ánh xạ các hostname không tồn tại đến máy chủ web chính của tên miền. Ví dụ, nếu chúng ta truy cập “idontexist.uit.edu.vn”, máy chủ DNS có thể ánh xạ nó thành địa chỉ IP của máy chủ web của “uit.edu.vn” và sau đó máy chủ web sẽ chuyển hướng bạn đến trang chính “www.uit.edu.vn”.

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

a. Rockyou

- Extract tập tin rockyou.txt

```
(ngoc@ngoc)-[~]
$ ls -lh /usr/share/wordlists/
total 51M
lrwxrwxrwx 1 root root 26 Oct 9 22:54 amass → /usr/share/amass/wordlists
lrwxrwxrwx 1 root root 25 Oct 9 22:54 dirb → /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root 30 Oct 9 22:54 dirbuster → /usr/share/dirbuster/w
ordlists
lrwxrwxrwx 1 root root 41 Oct 9 22:54 fasttrack.txt → /usr/share/set/src
/fasttrack/wordlist.txt
lrwxrwxrwx 1 root root 45 Oct 9 22:54 fern-wifi → /usr/share/fern-wifi-c
racker/extras/wordlists
lrwxrwxrwx 1 root root 28 Oct 9 22:54 john.lst → /usr/share/john/passwor
d.lst
lrwxrwxrwx 1 root root 27 Oct 9 22:54 legion → /usr/share/legion/wordlis
ts
lrwxrwxrwx 1 root root 46 Oct 9 22:54 metasploit → /usr/share/metasploit
-framework/data/wordlists
lrwxrwxrwx 1 root root 41 Oct 9 22:54 nmap.lst → /usr/share/nmap/nselib/
data/passwords.lst
-rw-r--r-- 1 root root 51M May 12 22:14 rockyou.txt.gz
lrwxrwxrwx 1 root root 39 Oct 9 22:54 sqlmap.txt → /usr/share/sqlmap/dat
a/txt/wordlist.txt
lrwxrwxrwx 1 root root 25 Oct 9 22:54 wfuzz → /usr/share/wfuzz/wordlist
lrwxrwxrwx 1 root root 37 Oct 9 22:54 wifite.txt → /usr/share/dict/wordl
ist-probable.txt

(ngoc@ngoc)-[~]
$ gunzip /usr/share/wordlists/rockyou.txt.gz
gzip: /usr/share/wordlists/rockyou.txt: Permission denied

(ngoc@ngoc)-[~]
$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
[sudo] password for ngoc:
```

- Danh sách các hostname thường gặp trong rockyou.txt

```
(ngoc@ngoc)-[~]
$ cat /usr/share/wordlists/rockyou.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
```

- Sử dụng Bash script để phân giải mỗi hostname có trong danh sách bằng rockyou.txt.

```
#!/bin/bash

# Kiểm tra xem file từ vựng có tồn tại không
if [ ! -f /usr/share/wordlists/rockyou.txt ]; then
    echo "File /usr/share/wordlists/rockyou.txt không tồn tại."
    exit 1
fi

# Duyệt qua danh sách từ vựng và phân giải DNS
while IFS= read -r word; do
    host "$word.megacorpone.com"
done < /usr/share/wordlists/rockyou.txt
```

- Một số hostname tìm được (vì file dài nên em chỉ liệt kê một số)

```
Host taylor13.megacorpone.com not found: 3(NXDOMAIN)
Host syracuse.megacorpone.com not found: 3(NXDOMAIN)
Host switchfoot.megacorpone.com not found: 3(NXDOMAIN)
support.megacorpone.com has address 51.222.169.218
Host soccer33.megacorpone.com not found: 3(NXDOMAIN)
Host soccer25.megacorpone.com not found: 3(NXDOMAIN)
Host sinatra.megacorpone.com not found: 3(NXDOMAIN)
Host sillygirl.megacorpone.com not found: 3(NXDOMAIN)
Host aleinad.megacorpone.com not found: 3(NXDOMAIN)
Host alcala.megacorpone.com not found: 3(NXDOMAIN)
Host akusayangkamu.megacorpone.com not found: 3(NXDOMAIN)
admin.megacorpone.com has address 51.222.169.208
Host VINCENT.megacorpone.com not found: 3(NXDOMAIN)
Host TYRONE.megacorpone.com not found: 3(NXDOMAIN)
Host SEXY123.megacorpone.com not found: 3(NXDOMAIN)
```

b. Seclists

- Danh sách các hostname thường gặp trong seclists

```
(ngoc@ngoc)-[~]
$ cat /usr/share/seclists/Discovery/DNS/namelist.txt
0
01
02
03
1
10
11
12
13
14
15
16
17
18
19
2
20
3
3com
4
5
6
7
8
9
a
a.auth-ns
a01
a02
a1
a2
aaademo
aaanalytics
aaaowa
```

- Sử dụng Bash script để phân giải mỗi hostname có trong danh sách bằng namelist.txt.

```
1#!/bin/bash
2
3# Kiểm tra xem file từ vựng có tồn tại không
4if [ ! -f /usr/share/seclists/Discovery/DNS/namelist.txt ]; then
5    echo "File /usr/share/wordlists/rockyou.txt không tồn tại."
6    exit 1
7fi
8
9# Duyệt qua danh sách từ vựng và phân giải DNS
10while IFS= read -r word; do
11    host "$word.megacorpone.com"
12done < /usr/share/seclists/Discovery/DNS/namelist.txt
13
```

Nhóm 18

- Một số hostname tìm được (vì file dài nên em chỉ liệt kê một số)

```
Host admgeothermie.megacorpone.com not found: 3(NXDOMAIN)
Host admgr.megacorpone.com not found: 3(NXDOMAIN)
Host admidentite.megacorpone.com not found: 3(NXDOMAIN)
admin.megacorpone.com has address 51.222.169.208
Host adminac.megacorpone.com not found: 3(NXDOMAIN)
Host adminapi.megacorpone.com not found: 3(NXDOMAIN)

Host bestworkplace.megacorpone.com not found: 3(NXDOMAIN)
Host besxpress.megacorpone.com not found: 3(NXDOMAIN)
Host bet.megacorpone.com not found: 3(NXDOMAIN)
beta.megacorpone.com has address 51.222.169.209
Host betaadmin.megacorpone.com not found: 3(NXDOMAIN)
Host betaapp.megacorpone.com not found: 3(NXDOMAIN)
Host betabattlestargalac.megacorpone.com not found: 3(NXDOMAIN)
```

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

- Sử dụng công cụ dig để tìm kiếm các nameserver cho các domain:

```
#!/bin/bash

# Kiểm tra xem có đủ tham số dòng lệnh hay không
if [ "$#" -eq 0 ]; then
    echo "Sử dụng: $0 domain1 domain2 ..."
    exit 1
fi

# Lặp qua danh sách các domain và liệt kê nameserver
for domain in "$@"; do
    echo "Nameserver cho domain $domain:"
    dig +short NS "$domain"
    echo
done
```

a. hcmus.edu.vn

- Thực thi chương trình với domain “hcmus.edu.vn”

```
(ngoc@ngoc)-[~] NXDOMAIN)
$ ./script3.sh hcmus.edu.vn
Nameserver cho domain hcmus.edu.vn:
dns2.hcmus.edu.vn. 3(NXDOMAIN)
dns1.hcmus.edu.vn. 3(NXDOMAIN)
server.hcmus.edu.vn. 0 DOMAIN)
one.com not found: 3(NXDOMAIN)
```

- Thực thi zone transfer trên các nameserver của “hcmus.edu.vn” nhưng bị từ chối.

```

└─(ngoc@ngoc)-[~]NXDOMAIN
$ host -l hcmus.edu.vn dns1.hcmus.edu.vn
;; Connection to 14.241.254.131#53(14.241.254.131) for hcmus.edu.vn failed:
timed out. Found: 3(NXDOMAIN)
;; Connection to 14.241.254.131#53(14.241.254.131) for hcmus.edu.vn failed:
timed out. Found: 3(NXDOMAIN)
;com not found: 3(NXDOMAIN)

└─(ngoc@ngoc)-[~]NXDOMAIN
$ host -l hcmus.edu.vn dns2.hcmus.edu.vn
;; Connection to 115.73.217.121#53(115.73.217.121) for hcmus.edu.vn failed:
timed out. Found: 3(NXDOMAIN)
;; Connection to 115.73.217.121#53(115.73.217.121) for hcmus.edu.vn failed:
timed out. Found: 3(NXDOMAIN)
;com not found: 3(NXDOMAIN)

└─(ngoc@ngoc)-[~]NXDOMAIN
$ host -l hcmus.edu.vn server.hcmus.edu.vn
Using domain server:
Name: server.hcmus.edu.vn
Address: 171.244.202.180#53
Aliases:
;com not found: 3(NXDOMAIN)
Host hcmus.edu.vn not found: 5(REFUSED)
; Transfer failed.

```

b. hcmussh.edu.vn

- Thực thi chương trình với domain “hcmussh.edu.vn”

```

└─(ngoc@ngoc)-[~]NXDOMAIN
$ ./script3.sh hcmussh.edu.vn
Nameserver cho domain hcmussh.edu.vn:
server.vnuhcm.edu.vn.
vnuserserv.vnuhcm.edu.vn.

```

- Thực thi zone transfer trên các nameserver của “hcmussh.edu.vn” nhưng bị từ chối.

```

└─(ngoc@ngoc)-[~]
$ host -l hcmussh.edu.vn server.vnuhcm.edu.vn
Using domain server:
Name: server.vnuhcm.edu.vn
Address: 103.88.121.201#53
Aliases:

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

└─(ngoc@ngoc)-[~]
$ host -l hcmussh.edu.vn vnuserserv.vnuhcm.edu.vn
Using domain server:
Name: vnuserserv.vnuhcm.edu.vn
Address: 103.88.121.200#53
Aliases:

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

```

c. uit.edu.vn

- Thực thi chương trình với domain “uit.edu.vn”

```
(ngoc@ngoc)-[~] NXDOMAIN
$ ./script3.sh uit.edu.vn
Nameserver cho domain uit.edu.vn:
ns2.pavietnam.vn. 3(NXDOMAIN)
ns1.pavietnam.vn. 3(NXDOMAIN)
nsbak.pavietnam.net.
zone.com.not.found: 3(NXDOMAIN)
```

- Thực thi zone transfer trên các nameserver của “uit.edu.vn” nhưng bị từ chối.

```
(ngoc@ngoc)-[~]
$ host -l uit.edu.vn ns1.pavietnam.vn
Using domain server:
Name: ns1.pavietnam.vn
Address: 112.213.89.3#53
Aliases:

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

(ngoc@ngoc)-[~]
$ host -l uit.edu.vn ns2.pavietnam.vn
Using domain server:
Name: ns2.pavietnam.vn
Address: 222.255.121.247#53
Aliases:

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

(ngoc@ngoc)-[~]
$ host -l uit.edu.vn nsbak.pavietnam.vn
Using domain server:
Name: nsbak.pavietnam.vn
Address: 112.213.89.3#53
Aliases:

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

d. hcmut.edu.vn

- Thực thi chương trình với domain “hcmut.edu.vn”

```
(ngoc@ngoc)-[~] NXDOMAIN
$ ./script3.sh hcmut.edu.vn
Nameserver cho domain hcmut.edu.vn:
dns3.hcmut.edu.vn. 3(NXDOMAIN)
dns2.hcmut.edu.vn. 3(NXDOMAIN)
dns4.hcmut.edu.vn. 3(NXDOMAIN)
dns1.hcmut.edu.vn. 3(NXDOMAIN)
zone.com.not.found: 3(NXDOMAIN)
```

- Thực thi zone transfer trên các nameserver của “hcmut.edu.vn” nhưng bị từ chối.

```

└─(ngoc@ngoc)─[~]
$ host -l hcmut.edu.vn dns1.hcmut.edu.vn
Using domain server:
Name: dns1.hcmut.edu.vn
Address: 101.99.31.218#53
Aliases:

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

└─(ngoc@ngoc)─[~]
$ host -l hcmut.edu.vn dns2.hcmut.edu.vn
Using domain server:
Name: dns2.hcmut.edu.vn
Address: 221.133.13.115#53
Aliases:

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

└─(ngoc@ngoc)─[~]
$ host -l hcmut.edu.vn dns3.hcmut.edu.vn
Using domain server:
Name: dns3.hcmut.edu.vn
Address: 203.205.32.235#53
Aliases:

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

└─(ngoc@ngoc)─[~]
$ host -l hcmut.edu.vn dns4.hcmut.edu.vn
;; Connection to 203.205.32.236#53(203.205.32.236) for hcmut.edu.vn failed:
timed out.
;; Connection to 203.205.32.236#53(203.205.32.236) for hcmut.edu.vn failed:
timed out.

```

e. hcmiu.edu.vn

- Thực thi chương trình với domain “hcmiu.edu.vn”

```

└─(ngoc@ngoc)─[~] NXDOMAIN
$ ./script3.sh hcmiu.edu.vn
Nameserver cho domain hcmiu.edu.vn:
hcm_server1.vnn.vn. (NXDOMAIN)
vdc-hn01.vnn.vn. (NXDOMAIN)

```

- Thực thi zone transfer trên các nameserver của “hcmiu.edu.vn” nhưng bị từ chối.

```
(ngoc@ngoc)-[~]
$ host -l hcmiu.edu.vn hcm-server1.vnn.vn
Using domain server:
Name: hcm-server1.vnn.vn
Address: 203.162.4.1#53
Aliases:

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

(ngoc@ngoc)-[~]
$ host -l hcmiu.edu.vn vdc-hn01.vnn.vn
Using domain server:
Name: vdc-hn01.vnn.vn
Address: 203.162.0.11#53
Aliases:

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

f. uel.edu.vn

- Thực thi chương trình với domain “uel.edu.vn”

```
(ngoc@ngoc)-[~]
$ ./script3.sh uel.edu.vn
Nameserver cho domain uel.edu.vn:
ns1.dns.net.vn.: 3(NXDOMAIN)
ns2.dns.net.vn.: 3(NXDOMAIN)
; com not found: 3(NXDOMAIN)
```

- Thực thi zone transfer trên các nameserver của “uel.edu.vn” nhưng bị từ chối.

```
(ngoc@ngoc)-[~]
$ host -l uel.edu.vn ns1.dns.net.vn
Using domain server:
Name: ns1.dns.net.vn
Address: 210.211.108.160#53
Aliases:

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

(ngoc@ngoc)-[~]
$ host -l uel.edu.vn ns2.dns.net.vn
Using domain server:
Name: ns2.dns.net.vn
Address: 103.45.229.100#53
Aliases:

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

g. hcmier.edu.vn

- Thực thi chương trình với domain “hcmier.edu.vn”

```
(ngoc@ngoc)-[~]NXDOMAIN
$ ./script3.sh hcmier.edu.vn
Nameserver cho domain hcmier.edu.vn:
server.vnuhcm.edu.vn.NXDOMAIN
vnuserv.vnuhcm.edu.vn.NXDOMAIN
pone.com not found: 3(NXDOMAIN)
```

- Thực thi zone transfer trên các nameserver của “hcmier.edu.vn” nhưng bị từ chối.

```
(ngoc@ngoc)-[~]
$ host -l hcmier.edu.vn server.vnuhcm.edu.vn
Using domain server:
Name: server.vnuhcm.edu.vn
Address: 103.88.121.201#53
Aliases:

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

(ngoc@ngoc)-[~]
$ host -l hcmier.edu.vn vnuserv.vnuhcm.edu.vn
Using domain server:
Name: vnuserv.vnuhcm.edu.vn
Address: 103.88.121.200#53
Aliases:

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

h. vnuhcm.edu.vn

- Thực thi chương trình với domain “vnuhcm.edu.vn”

```
(ngoc@ngoc)-[~]NXDOMAIN
$ ./script3.sh vnuhcm.edu.vn
Nameserver cho domain vnuhcm.edu.vn:
ns1.vdc2.vn.NXDOMAIN
vnuserv.vnuhcm.edu.vn.NXDOMAIN
server.vnuhcm.edu.vn.NXDOMAIN
ns2.vdc2.vn.NXDOMAIN
```

- Thực thi zone transfer trên các nameserver của “vnuhcm.edu.vn”.

```

└─(ngoc㉿ngoc) [~] ~: 3(NXDOMAIN)
$ host -l vnuhcm.edu.vn ns1.vdc2.vn
Using domain server:
Name: ns1.vdc2.vn 3(NXDOMAIN)
Address: 14.225.232.25#53
Aliases:
Host vnuhcm.edu.vn not found: 5(REFUSED)
; Transfer failed. 3(NXDOMAIN)
└─(ngoc㉿ngoc) [~] NXDOMAIN
$ host -l vnuhcm.edu.vn vnuserv.vnuhcm.edu.vn
Using domain server: 3(NXDOMAIN)
Name: vnuserv.vnuhcm.edu.vn 3(NXDOMAIN)
Address: 103.88.121.200#53 3(NXDOMAIN)
Aliases:
Host vnuhcm.edu.vn not found: 5(REFUSED)
; Transfer failed. 3(NXDOMAIN)
└─(ngoc㉿ngoc) [~] NXDOMAIN
$ host -l vnuhcm.edu.vn server.vnuhcm.edu.vn
Using domain server:
Name: server.vnuhcm.edu.vn 3(NXDOMAIN)
Address: 103.88.121.201#53 3(NXDOMAIN)
Aliases:
Host vnuhcm.edu.vn not found: 5(REFUSED)
; Transfer failed. 3(NXDOMAIN)
└─(ngoc㉿ngoc) [~] NXDOMAIN
$ host -l vnuhcm.edu.vn ns2.vdc2.vn
Using domain server:
Name: ns2.vdc2.vn
Address: 14.225.232.26#53
Aliases:
vnuhcm.edu.vn has address 103.88.121.29
vnuhcm.edu.vn name server vnuserv.vnuhcm.edu.vn.
vnuhcm.edu.vn name server server.vnuhcm.edu.vn.
www.4s.vnuhcm.edu.vn has address 118.69.204.199
aaa.vnuhcm.edu.vn has address 103.88.123.21
aaa1.vnuhcm.edu.vn has address 103.88.123.22
aad.vnuhcm.edu.vn has address 203.162.44.60
ab.vnuhcm.edu.vn has address 203.162.147.252
aun.vnuhcm.edu.vn has address 203.162.147.168
baixektx.vnuhcm.edu.vn has address 123.30.236.140
baocaoaad.vnuhcm.edu.vn has address 203.162.44.60
mssql.baocaoaad.vnuhcm.edu.vn has address 203.162.44.60
betaaad.vnuhcm.edu.vn has address 222.255.69.252
cdio2015.vnuhcm.edu.vn has address 221.133.13.127
cea.vnuhcm.edu.vn has address 103.88.123.7
csgd.cea.vnuhcm.edu.vn has address 103.88.123.7
database.cea.vnuhcm.edu.vn has address 103.88.123.7
dkht.cea.vnuhcm.edu.vn has address 103.88.123.7
cete.vnuhcm.edu.vn has address 103.88.123.2
chrd.vnuhcm.edu.vn has address 203.162.147.149
club.vnuhcm.edu.vn has address 203.162.147.185
www.cntttt.vnuhcm.edu.vn has address 203.162.44.72
congdoan.vnuhcm.edu.vn has address 118.69.123.142
cpmu-demo.vnuhcm.edu.vn has address 103.88.121.59
cpmu-demo1.vnuhcm.edu.vn has address 112.78.11.146
cps.vnuhcm.edu.vn has address 112.78.11.146
ct.vnuhcm.edu.vn has address 203.162.147.252
data.vnuhcm.edu.vn has address 203.162.147.185

```

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

- Standard Enumeration (std): Loại này sử dụng các truy vấn DNS tiêu chuẩn để thu thập thông tin về tên miền, chẳng hạn như các bản ghi DNS chính (A, MX, NS, SOA, TXT).


```
dnsrecon -t std
```
- Brute Force Enumeration (brt): Loại này sử dụng tấn công "brute force" để tìm kiếm tất cả các bản ghi DNS có thể của tên miền.


```
dnsrecon -t brt
```
- Reverse DNS Enumeration (rev): Sử dụng tùy chọn này để thực hiện enumeration ngược (reverse enumeration) để xác định tên miền của một địa chỉ IP.


```
dnsrecon -t rev
```
- Zone Transfer Enumeration (axfr): Loại này thực hiện kiểm tra khả năng chuyển dữ liệu vùng (zone transfer) từ máy chủ DNS. Điều này có thể cho phép thu thập nhiều thông tin về tên miền, bao gồm danh sách các máy chủ con.


```
dnsrecon -t axfr
```
- Reverse Lookup Enumeration (rvl): Sử dụng tùy chọn này để thực hiện tìm kiếm đảo ngược (reverse lookup) để tìm các địa chỉ IP liên quan đến tên miền.


```
dnsrecon -t rvl
```
- Top Level Domain (tld): Thực hiện enumeration trên các tên miền cấp cao nhất (TLD) như ".com," ".net," ".org," v.v.


```
dnsrecon -t tld
```

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

- Thực hiện Reverse DNS Enumeration cho một phạm vi dải địa chỉ IP: Điều này sẽ thực hiện Reverse DNS Enumeration cho các địa chỉ IP trong dải từ "38.100.193.0" đến "38.100.193.255"

```
(ngoc@ngoc)-[~]
$ dnsrecon -t rvl -r 38.100.193.0/24
[*] Performing Reverse Lookup from 38.100.193.0 to 38.100.193.255
[+] PTR syslog.megacorpone.com 38.100.193.66
[+] PTR beta.megacorpone.com 38.100.193.69
[+] PTR ns1.megacorpone.com 38.100.193.70
[+] PTR admin.megacorpone.com 38.100.193.72
[+] PTR mail2.megacorpone.com 38.100.193.73
[+] PTR www.megacorpone.com 38.100.193.76
[+] PTR vpn.megacorpone.com 38.100.193.77
[+] PTR ns2.megacorpone.com 38.100.193.80
[+] PTR mail.megacorpone.com 38.100.193.84
[+] PTR snmp.megacorpone.com 38.100.193.85
[+] PTR siem.megacorpone.com 38.100.193.89
[+] PTR router.megacorpone.com 38.100.193.91
[+] PTR ns3.megacorpone.com 38.100.193.90
```

- Kết hợp Standard Enumeration và Zone Transfer Enumeration cho tên miền cụ thể: Điều này sẽ thực hiện cả Standard Enumeration và kiểm tra khả năng chuyển dữ liệu vùng (zone transfer) cho tên miền "megacorpone.com."

```
(ngoc@ngoc) - [~]
$ dnsrecon -t std -t axfr -d megacorpone.com
[*] Checking for Zone Transfer for megacorpone.com name servers
[*] Resolving SOA Record
[+] SOA ns1.megacorpone.com 51.79.37.18
[*] Resolving NS Records
[*] NS Servers found:
[+] NS ns2.megacorpone.com 51.222.39.63
[+] NS ns3.megacorpone.com 66.70.207.180
[+] NS ns1.megacorpone.com 51.79.37.18
[*] Removing any duplicate NS server IP Addresses ...
[*]
[*] Trying NS server 66.70.207.180
[+] 66.70.207.180 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server 51.222.39.63
[+] 51.222.39.63 Has port 53 TCP Open
[+] Zone Transfer was successful !!
[*] NS ns1.megacorpone.com 51.79.37.18
[*] NS ns2.megacorpone.com 51.222.39.63
[*] NS ns3.megacorpone.com 66.70.207.180
[*] TXT Try Harder
[*] TXT google-site-verification=U7B_b0HNeBtY4qYGQZNsEYXFCJ32hMNV3GtC0
wWq5pA
```

28. So sánh 2 công cụ DNSEnum và DNSRecon? Công cụ nào dễ sử dụng hơn? Công cụ nào cho kết quả chính xác hơn? Công cụ nào hiển thị nhiều kết quả hơn?

DNSEnum và DNSRecon là cả hai công cụ phổ biến được sử dụng để thực hiện enumeration và thu thập thông tin về DNS. Dưới đây là bảng so sánh giữa chúng:

| Tiêu chí | DNSEnum | DNSRecon |
|---------------------|---|--|
| Độ khó | DNSEnum thường được coi là dễ sử dụng hơn và phù hợp cho người mới bắt đầu trong việc kiểm tra tên miền và enumeration DNS. Nó cung cấp một giao diện dòng lệnh đơn giản và có ít tùy chọn. | DNSRecon cung cấp nhiều tùy chọn và tính năng mạnh mẽ, nhưng có thể đòi hỏi kiến thức kỹ thuật hơn để sử dụng hiệu quả. Do đó, nó có thể có một học hỏi cao hơn so với DNSEnum. |
| Độ chính xác | DNSEnum tập trung vào việc thu thập thông tin cơ bản về DNS và tên miền, như các bản ghi DNS chính. Điều này có thể dẫn đến kết quả đơn giản hơn. | DNSRecon có nhiều tùy chọn và module enumeration khác nhau, cho phép bạn tùy chỉnh kiểm tra của mình. Điều này có thể cho phép bạn thu thập nhiều thông tin hơn, nhưng yêu cầu kiến thức và kỹ năng cao hơn để cấu hình. |
| Hiển thị | DNSEnum thường trả về kết quả trong định dạng đơn giản, dễ đọc. Nó hiển thị thông tin cơ bản về DNS và tên miền một cách rõ ràng. | DNSRecon có thể hiển thị nhiều kết quả hơn bởi vì nó cung cấp nhiều module enumeration và tùy chọn. Kết quả có thể phức tạp hơn và cần sắp xếp và phân tích cẩn thận. |

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

- Dùng Nmap scan port của máy kali

```
(ngoc@ngoc)-[~]
$ sudo nmap -sS 192.168.184.133
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 00:25 +07
Nmap scan report for 192.168.184.133
Host is up (0.0000050s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

- Dùng wireshark để bắt gói tin

| | | | | |
|----------------|-----------------|-----------------|-----|--|
| 33 5.419998011 | 192.168.184.133 | 192.168.184.133 | TCP | 60 37726 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 34 5.420010729 | 192.168.184.133 | 192.168.184.133 | TCP | 60 80 → 37726 [SYN, ACK] Seq=0 Ack=1 Win=65495 Len=0 MSS=65495 |
| 35 5.420013200 | 192.168.184.133 | 192.168.184.133 | TCP | 56 37726 → 80 [RST] Seq=1 Win=0 Len=0 |

- Mô tả quá trình gửi và nhận khi thực hiện SYN Scan:

- Bước 1: 192.168.184.133:37726 khởi tạo gói tin SYN (Synchronize)

Quá trình SYN Scan bắt đầu bằng việc gửi một loạt gói tin có cờ SYN đến máy chủ đích trên các cổng mục tiêu. Gói tin SYN đóng vai trò như một yêu cầu mở kết nối TCP.
- Bước 2: 192.168.184.133:80 phản hồi SYN-ACK (Synchronize-Acknowledgment):

Vì cổng 80 trên máy chủ đích đang mở nên nó sẽ phản hồi bằng một gói tin SYN-ACK để xác nhận yêu cầu kết nối TCP.
- Bước 3: 192.168.184.133:37726 phản hồi RST (Reset):

Máy nguồn gửi phản hồi đã nhận được gói SYN-ACK, quá trình bắt tay ba bước kết thúc.

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

- Dùng Nmap để thực hiện TCP Connect Scan

```
(ngoc@ngoc)-[~]
$ sudo nmap -sT 192.168.184.133
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 00:37 +07
Nmap scan report for 192.168.184.133
Host is up (0.00012s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http

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

- Dùng wireshark để bắt gói tin

| | | | | |
|----------------|-----------------|-----------------|-----|---|
| 19 3.241569508 | 192.168.184.133 | 192.168.184.133 | TCP | 76 38198 → 80 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TStamp=3461394524 TSecr=0 WS=128 |
| 20 3.241586284 | 192.168.184.133 | 192.168.184.133 | TCP | 76 80 → 38198 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TStamp=3461394524 TSecr=3461394524 |
| 21 3.241683902 | 192.168.184.133 | 192.168.184.133 | TCP | 68 38198 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TStamp=3461394524 TSecr=3461394524 |

- Mô tả quá trình gửi và nhận khi thực hiện TCP Connect Scan:

- Bước 1: 192.168.184.133:38198 khởi tạo gói tin SYN (Synchronize):

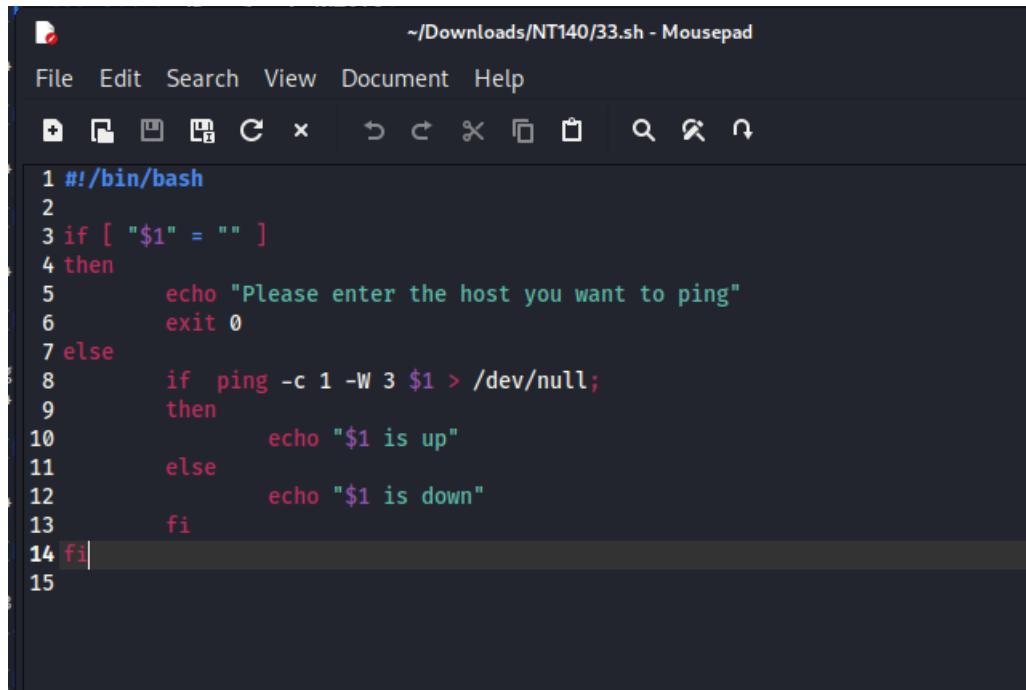
Máy quét (Nmap) gửi một gói tin có cờ SYN đến máy chủ đích để bắt đầu quá trình thiết lập kết nối.
- Bước 2: 192.168.184.133:80 phản hồi gói tin SYN-ACK (Synchronize-Acknowledgment):

Nếu cổng trên máy chủ đích đang mở và máy chủ đích lắng nghe, nó sẽ phản hồi bằng một gói tin có cờ SYN và ACK để xác nhận yêu cầu kết nối và đồng thời xác nhận rằng máy chủ đích đồng ý thiết lập kết nối TCP.

- Bước 3: 192.168.184.133:38198 phản hồi gói tin ACK (Acknowledgment): Máy quét (Nmap) sau đó gửi một gói tin có cờ ACK để xác nhận kết nối đã được thiết lập.

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

- Chương trình Bash script: kiểm tra 1 host có đang hoạt động không

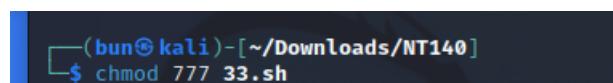


```

#!/bin/bash
if [ "$1" = "" ]
then
    echo "Please enter the host you want to ping"
    exit 0
else
    if ping -c 1 -W 3 $1 > /dev/null;
    then
        echo "$1 is up"
    else
        echo "$1 is down"
    fi
fi

```

- Cấp quyền cho file 33.sh



```

$ chmod 777 33.sh

```

- Chạy chương trình ở terminal



```

$ ./33.sh 8.8.8.8
8.8.8.8 is up

$ ./33.sh 127.0.0.1
127.0.0.1 is up

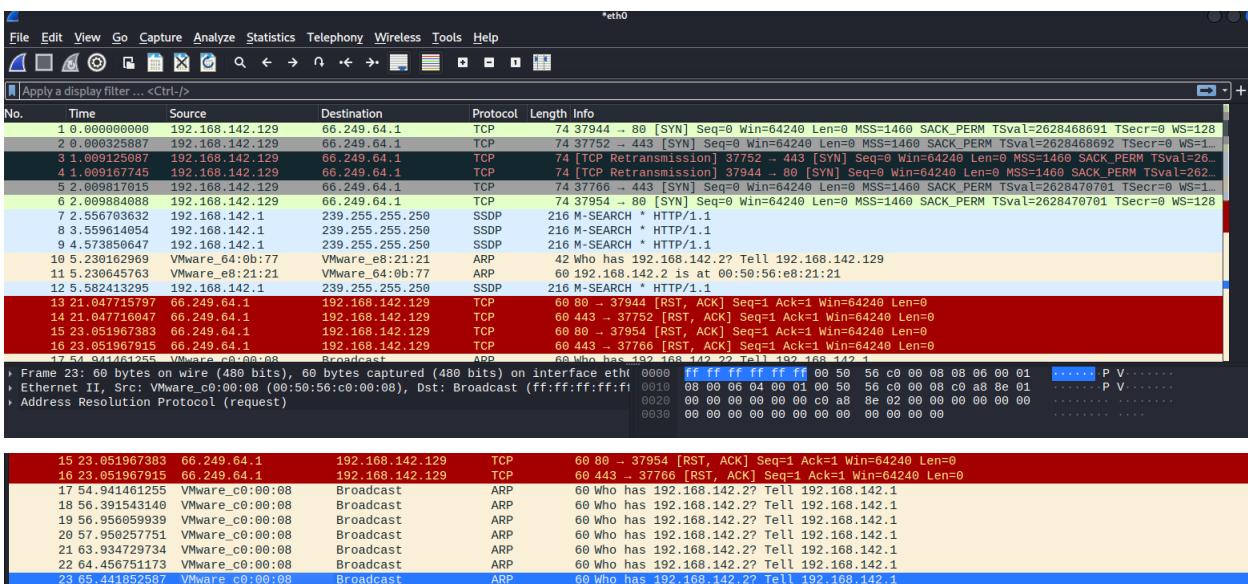
$ ./33.sh 0.0.0.1
0.0.0.1 is down

```

33. Sử dụng Wireshark để phân tích gói tin khi sử dụng Nmap với tùy chọn -sn
- ping tới 66.249.64.1 (1 IP của Googlebot)

```
(bun㉿kali)-[~]
$ nmap -v -sn 66.249.64.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 20:07 +07
Initiating Ping Scan at 20:07
Scanning 66.249.64.1 [2 ports]
Completed Ping Scan at 20:07, 3.02s elapsed (1 total hosts)
Nmap scan report for 66.249.64.1 [host down]
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.02 seconds
```

- Phân tích bằng Wireshark



- Nhận xét:

nmap với tùy chọn -sn: gửi 2 gói tin TCP SYN tới port 80 và 443 của host

Sau khi nhận được các gói tin TCP SYN thì host phản hồi lại bằng cách gửi lại 2 gói tin TCP ACK tới port 80 và 443 của máy đã gửi gói tin TCP SYN.

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

- Máy Metasploitable 2 đang hoạt động trên ip 192.168.184.137

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:dd:98:5e
          inet addr:192.168.184.137 Bcast:192.168.184.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fedd:985e/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:64 errors:0 dropped:0 overruns:0 frame:0
             TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:5912 (5.7 KB) TX bytes:6814 (6.6 KB)
             Interrupt:17 Base address:0x2000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
             UP LOOPBACK RUNNING MTU:16436 Metric:1
             RX packets:96 errors:0 dropped:0 overruns:0 frame:0
             TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:21437 (20.9 KB) TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$ _
```

- Kiểm tra các banner của dịch vụ (-sV) và chạy các script khám phá hệ điều hành và dịch vụ (-A)

```
(ngoc@ngoc)-[~]
$ nmap -sV -sT -A 192.168.184.137
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 21:58 +07
Nmap scan report for 192.168.184.137
Host is up (0.0014s latency).

Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|_STAT:  Metasploitable.nvr  Metasploitable.vm  Metasploitable.vm
| FTP server status:
|   Connected to 192.168.184.133
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp         Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2 DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2 DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|   ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
```

- Các banner, dịch vụ đang chạy trên máy Metasploitable 2:

- TCP FTP

```
21/tcp open  ftp          vsftpd 2.3.4
| ftp-syst:
|_ STAT:
|   FTP server status:
|     Connected to 192.168.184.133
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

- TCP SSH

```
22/tcp open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
```

- TCP SSH

```
22/tcp open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
```

- TCP Telnet

```
23/tcp open  telnet       Linux telnetd
```

- TCP SMTP

```
25/tcp open  smtp         Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_  SSL2_RC2_128_CBC_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2023-10-26T14:58:56+00:00; 0s from scanner time.
```

- TCP Domain

```
53/tcp open  domain      ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
```

- TCP HTTP

```
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
|   program version port/proto service
|   100000 2          111/tcp   rpcbind
|   100000 2          111/udp   rpcbind
|   100003 2,3,4    2049/tcp   nfs
|   100003 2,3,4    2049/udp   nfs
|   100005 1,2,3    48983/tcp  mountd
|   100005 1,2,3    52293/udp mountd
|   100021 1,3,4    39426/udp nlockmgr
|   100021 1,3,4    49583/tcp nlockmgr
|   100024 1        47418/udp status
|_ 100024 1        52780/tcp status
```

- Và một số dịch vụ khác

```
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open Detbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec      netkit-rsh rexecd
513/tcp open login     OpenBSD or Solaris rlogind
514/tcp open tcpwrapped
1099/tcp open java-rmi  GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs      2-4 (RPC #100003)
2121/tcp open ftp      ProFTPD 1.3.1
3306/tcp open mysql    MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: Speaks41ProtocolNew, ConnectWithDatabase, LongColumnFlag, Support41Auth, SupportsTransactions, SupportsCompression, SwitchToSSLAfterHandshake
|   Status: Autocommit
|_ Salt: }n/-d2h7xvi,>4(kf;4
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: 2023-10-26T14:58:56+00:00; 0s 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
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
```

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

- Sử dụng NSE script để kiểm tra dịch vụ HTTP: Để kiểm tra cụ thể các lỗ hổng trên dịch vụ HTTP trên Metasploitable 2, bạn có thể sử dụng kịch bản http-vuln-cve2014-3704.

```
(ngoc@ngoc)-[~]
$ nmap -p 80,443 --script http-vuln-cve2014-3704 192.168.184.137
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 22:19 +07
Nmap scan report for 192.168.184.137
Host is up (0.00045s latency).

PORT      STATE SERVICE
80/tcp    open  http
443/tcp   closed https

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

- Sử dụng NSE script để kiểm tra lỗ hổng Samba.

```
(ngoc@ngoc)-[~]
$ nmap -p 139,445 --script smb-vuln* 192.168.184.137
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 22:22 +07
Nmap scan report for 192.168.184.137
Host is up (0.00049s latency).

PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Host script results:
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false

Nmap done: 1 IP address (1 host up) scanned in 6.12 seconds
```