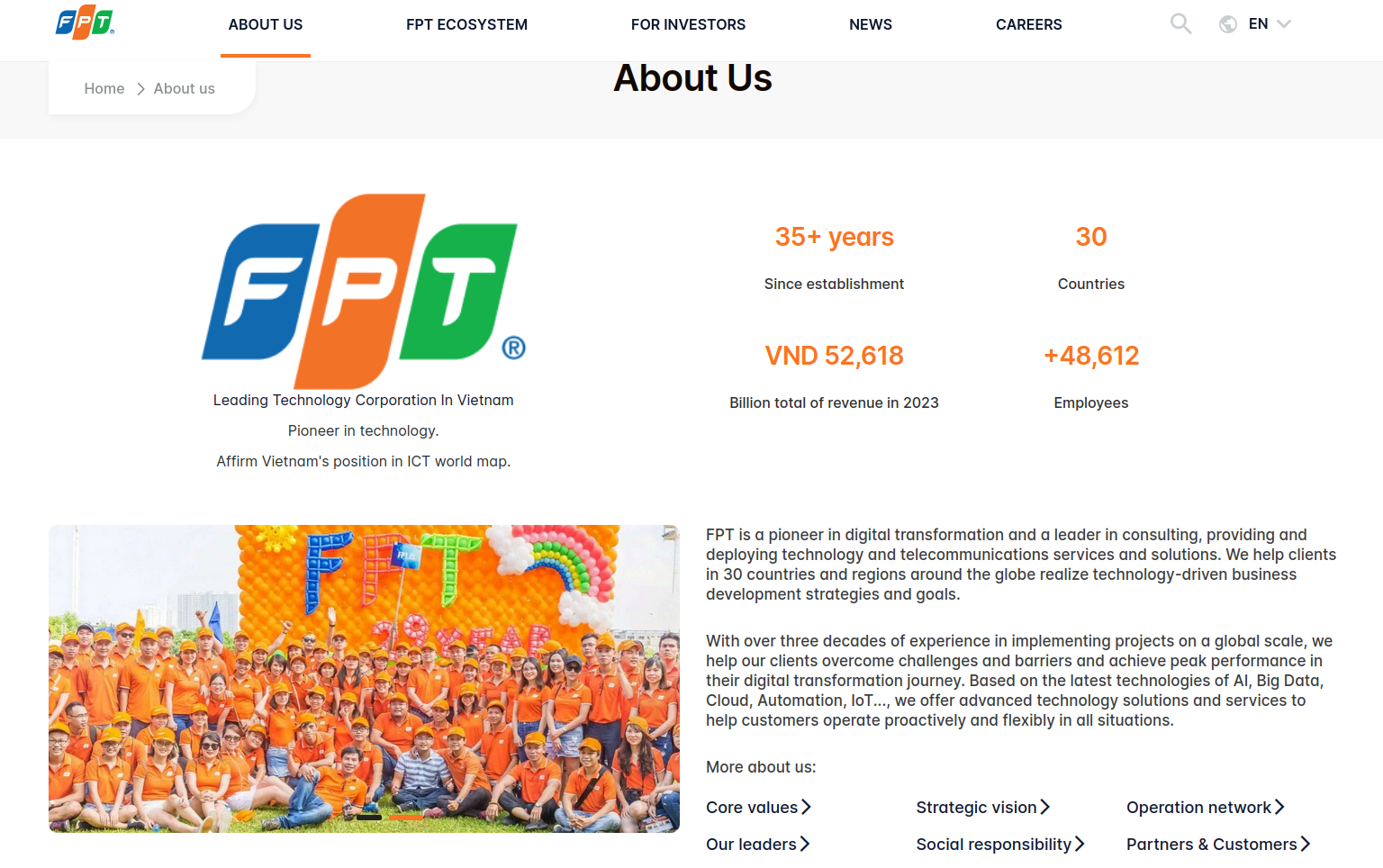
1. MY WORKFLOW

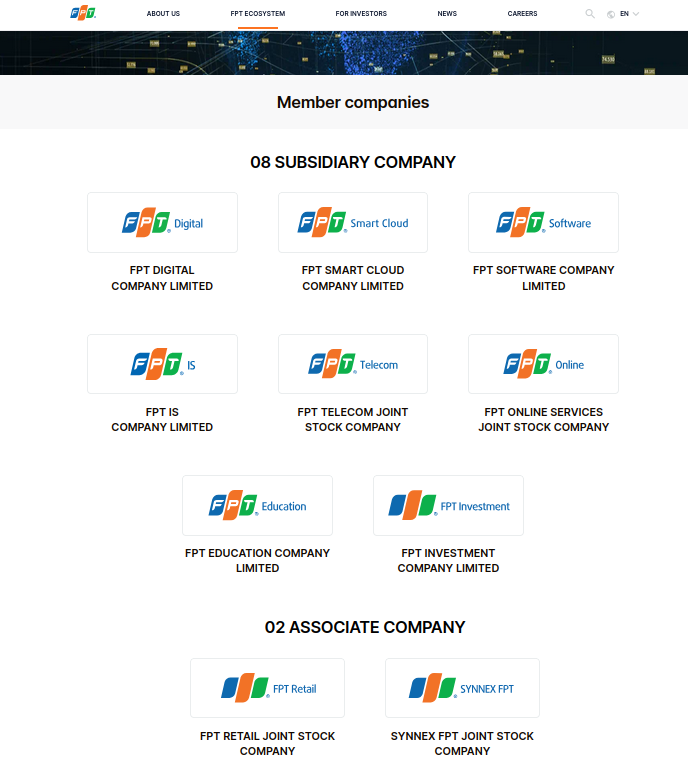
*\*Thứ tự các nội dung được báo cáo không được sắp xếp theo như trong module đào tạo.*

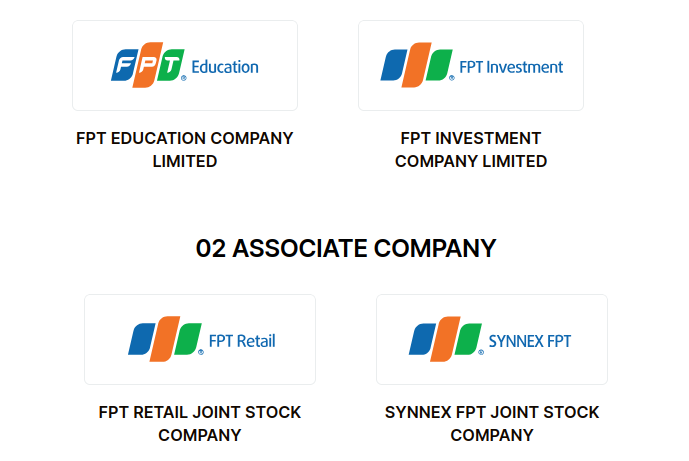
- Trước tiên, tôi không biết thông tin gì về mục tiêu ngoài tên. Tôi thực hiện tìm kiếm trên các công cụ tra cứu như Google/Yandex/Baidu/… để nắm được các thông tin cơ bản của mục tiêu.



→ Đây là tập đoàn lớn, đa quốc gia trong lĩnh vực chuyển đổi số, công nghệ thông tin và viễn thông.

- Sau một hồi “thăm quan” [https://fpt.com](https://fpt.com/), tôi tìm thấy mục Member companies. Đây sẽ là nội dung thích hợp để tìm kiếm các đơn vị con trong tập đoàn cùng với các domain liên quan!





→ Thông qua từng box giới thiệu các công ty/tổ chức trực thuộc, tôi có được một số Domain ban đầu như:

* https://digital.fpt.com.vn/
* https://fptsmartcloud.com/
* https://fptsoftware.com/
* https://fpt-is.com/
* https://fpt.vn/
* https://fptonline.net/
* https://fpt.edu.vn/
* https://fptcapital.com.vn/
* https://fptshop.com.vn/
* https://nhathuoclongchau.com/ *(SSL cert hết hạn) → 403*
* https://nhathuoclongchau.com.vn/
* https://synnexfpt.com/

- Ngoài ra, tôi sử dụng crt.sh để tìm kiếm các SSL cert có thông tin liên quan đến tên mục tiêu “fpt”(các keywords như “fptsoftware”, “fptsmartcloud”… không có kết quả):

→ Nhận được kết quả, dùng một chút JS đế lọc các cert sẽ hết hạn trong năm 2024 và 2025:

→ Kết hợp với các domain từ Member companies, tôi đã có được danh sách domain/fqdn ban đầu cho giai đoạn External Reconnaissance!

* 1. Passive Recon Techniques
     1. Gathering Domain IP/DNS Information
        1. Host utility

- Dùng command “**for domain in $(cat ./domain.txt); do host $domain >> host.txt; done**” với các công cụ không hỗ trợ pipeline thì tôi dùng *bash for* để thực thi công cụ với danh sách Domain hoặc dùng với *xargs*.

- Thử xem các domain không có kết quả “**grep "not found" host.txt**”:

- Lọc danh sách domain + ip “**grep "has addr" host.txt | awk '{print $1 "\t" $NF}' | tee host\_domain\_ip.txt**”:

- Lọc danh sách domain + mail server “**grep "handle" host.txt | awk '{print $1 "\t" $NF}' | tee host\_domain\_mail.txt**”

* + - 1. Nslookup

- Lấy thông tin IP với nslookup “**cat domain.txt | nslookup | tee nslookup**”

- Ngoài ra, thử truy vấn với server 1.1.1.1 và 8.8.8.8: “**cat domain.txt | nslookup - 1.1.1.1 | tee nslookup1111**”, “**cat domain.txt | nslookup - 8.8.8.8 | tee nslookup8888**”

→ Thử so sánh thì kết quả của cả ba là giống nhau!

* + - 1. DNSRecon
      2. Dig
    1. WAF (Web Application Firewall) Detection With Wafw00f
    2. Gathering Domain/Website Information
       1. Whois information
       2. Netcraft Site Report
       3. DNS Dumpster
       4. Discovering Web Technologies With WhatWeb
       5. Browser Add-ons
    3. Gathering Employee Information
       1. Gathering Employee Emails With theHarvester
    4. Passive Subdomain Enumeration With Sublist3r
    5. Subdomain Enumeration With Google Dorks
  1. Active Recon Techniques
     1. DNS Zone Transfers
        1. DNS Zone Transfer With DNSRecon
        2. DNS Zone Transfer With Fierce
     2. Subdomain Brute-force
        1. Subdomain Brute-force with Knockpy
     3. Port Scanning
        1. Port Scanning With Nmap
        2. Nmap Stealth Scan
        3. Nmap Script Scan
     4. Directory Brute-Force
        1. Directory Brute-Force With Gobuster
     5. Website Vulnerability Scanning
        1. Website Vulnerability Scanning With Nikto
        2. CMS Vulnerability Scanning
  2. Automated Recon Frameworks
     1. Automated Recon With Sn1per
     2. Automated Recon With OWASP Amass