

# BÁO CÁO THỰC HÀNH

Môn học: Bảo mật web và ứng dụng

Lab 3: Reconnaissance

GVHD: Nghi Hoàng Khoa

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.P11.ATCL.1

STT	Họ và tên	MSSV	Email
1	Võ Sỹ Minh	21521146	21521146@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Công việc	Kết quả tự đánh giá
1	Bài tập về nhà	90%

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

---

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

## BÁO CÁO CHI TIẾT

- Tìm kiếm các tên miền phụ của \*.uit.edu.vn

Sử dụng tính năng của VirusTotal

Subdomains (151) ⓘ					
oms.uit.edu.vn	0 / 94	45.122.249.78	118.69.123.140		
mail.uit.edu.vn	0 / 94	209.85.200.121	209.85.145.121	74.125.69.121	
gn.uit.edu.vn	0 / 94	45.122.249.78	118.69.123.140		
ngayphapluat.uit.edu.vn	0 / 94	45.122.249.78	118.69.123.140		
daihoiviii-tuoitre.uit.edu.vn	0 / 94	45.122.249.78	118.69.123.140		
openvpn.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78		
rms.uit.edu.vn	0 / 94	45.122.249.78	118.69.123.140		
dttt.uit.edu.vn	0 / 94	45.122.249.78	118.69.123.140		
cbsv1.uit.edu.vn	0 / 94	172.66.44.191	172.66.47.65		
tuyensinhsdh.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78		
dreamspark.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78		
cd.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78		
smtp.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78		
live.uit.edu.vn	0 / 94	42.116.11.16			
uhongdl.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78		
gaingon.uit.edu.vn	0 / 94	45.122.249.78	118.69.123.140		
traibao.uit.edu.vn	0 / 94	45.122.249.78	118.69.123.140		
daa1.uit.edu.vn	0 / 94	45.122.249.78	118.69.123.140		
dkhpapi.uit.edu.vn	0 / 94	45.122.249.75	118.69.123.137		
dsc.uit.edu.vn	0 / 94	192.0.78.13	192.0.78.12	118.69.123.140	...
elearning.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78		

Sử dụng c99.nl:

Result of uit.edu.vn

https://subdomainfinder.c99.nl/scans/2024-10-26/uit.edu.vn

Scan date: 2024-10-26 18:07:00  
 Domain Country: Vietnam (VN) 🇻🇳  
 Subdomains found: 38  
 Most used IP: 45.122.249.78 (19x)

Whois Check Check Status Copy to clipboard Download CSV Download JSON

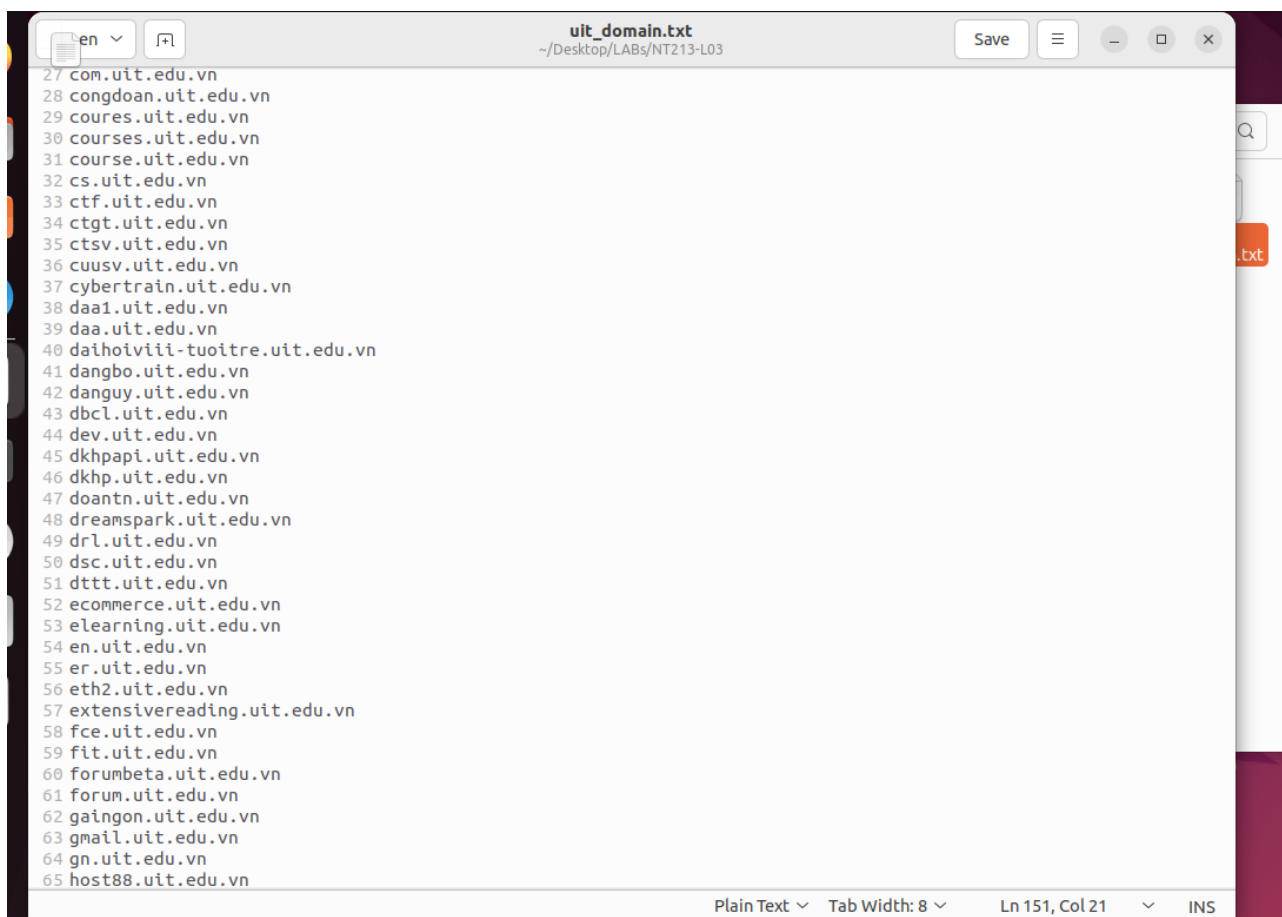
Subdomain	IP	Cloudflare
519bb137df6144dcbda18e87d53ad8a-0-s-80.vlab.uit.edu.vn	45.122.249.74	☁️
a084742fa316491c8c78564efcbce9e0-68f6236f-vm-80.vlab2.uit.edu.vn	45.122.249.76	☁️
annotation.mmlab.uit.edu.vn	118.69.123.140	☁️
api.mmlab.uit.edu.vn	45.122.249.78	☁️
app.tech4covid.uit.edu.vn	118.69.123.140	☁️
app1.iot.uit.edu.vn	45.122.249.78	☁️
app2.iot.uit.edu.vn	118.69.123.140	☁️
cbsv1.uit.edu.vn	172.66.44.191	☁️
competitions.uit.edu.vn	45.122.249.78	☁️
console-cloud.vlab.uit.edu.vn	45.122.249.74	☁️
console-cloud.vlab2.uit.edu.vn	45.122.249.76	☁️
cs.uit.edu.vn	45.122.249.78	☁️
dsc.uit.edu.vn	192.0.78.12	☁️
eth2.uit.edu.vn	42.116.11.19	☁️
hmcovidsafe-dev-gw.tech4covid.uit.edu.vn	45.122.249.78	☁️

- **Tìm kiếm các địa chỉ IP thuộc \*.uit.edu.vn và các cổng đang mở tương ứng.**

Có thể sử dụng các thông tin dò được ở trên vì chứa các địa chỉ IP tương ứng. Hoặc sử dụng lệnh tương tự với rmit.edu.vn làm ở trên.

Từ đó lưu các IP để dò port

Bước đầu lấy các sub domain bên trên



```
27 com.uit.edu.vn
28 congdoan.uit.edu.vn
29 coures.uit.edu.vn
30 courses.uit.edu.vn
31 course.uit.edu.vn
32 cs.uit.edu.vn
33 ctf.uit.edu.vn
34 ctgt.uit.edu.vn
35 ctsv.uit.edu.vn
36 cuusv.uit.edu.vn
37 cybertrain.uit.edu.vn
38 daa1.uit.edu.vn
39 daa.uit.edu.vn
40 daihoiviii-tuoitre.uit.edu.vn
41 dangbo.uit.edu.vn
42 danguy.uit.edu.vn
43 dbcl.uit.edu.vn
44 dev.uit.edu.vn
45 dkhpapi.uit.edu.vn
46 dkhp.uit.edu.vn
47 doantn.uit.edu.vn
48 dreamspark.uit.edu.vn
49 drl.uit.edu.vn
50 dsc.uit.edu.vn
51 dttt.uit.edu.vn
52 ecommerce.uit.edu.vn
53 elearning.uit.edu.vn
54 en.uit.edu.vn
55 er.uit.edu.vn
56 eth2.uit.edu.vn
57 extensivereading.uit.edu.vn
58 fce.uit.edu.vn
59 fit.uit.edu.vn
60 forumbeta.uit.edu.vn
61 forum.uit.edu.vn
62 gaingon.uit.edu.vn
63 gmail.uit.edu.vn
64 gn.uit.edu.vn
65 host88.uit.edu.vn
```

Phân giải IP:

```
simon@minh-1146:~/Desktop/LABs/NT213-L03$ cat resolveIP.sh
#!/bin/bash
for host in $(cat uit_domain.txt); do
    printf "%s\n" $(resolveip -s "$host") >> uit.txt
done
```

1	118.69.123.140
2	142.250.197.147
3	172.66.44.191
4	192.0.78.12
5	192.0.78.13
6	42.116.11.16
7	42.116.11.19
8	45.122.249.74
9	45.122.249.75
10	45.122.249.76
11	45.122.249.78

Dò cổng:

```

simon@minh-1146:~/Desktop/LABs/NT213-L03$ cat scanPort.sh
#!/bin/bash

ports=$(cat port.txt)

echo "IP,Port,State" > uit_results.csv

while IFS= read -r ip; do
    echo "Đang quét các cổng $ports cho IP: $ip"

    nmap -p "$ports" "$ip" | grep 'open|closed|filtered' | while read -r line;
    do
        port=$(echo "$line" | awk '{print $1}' | cut -d '/' -f1)
        state=$(echo "$line" | awk '{print $2}')
        echo "$ip,$port,$state" >> uit_results.csv
    done
done < uitIP.txt

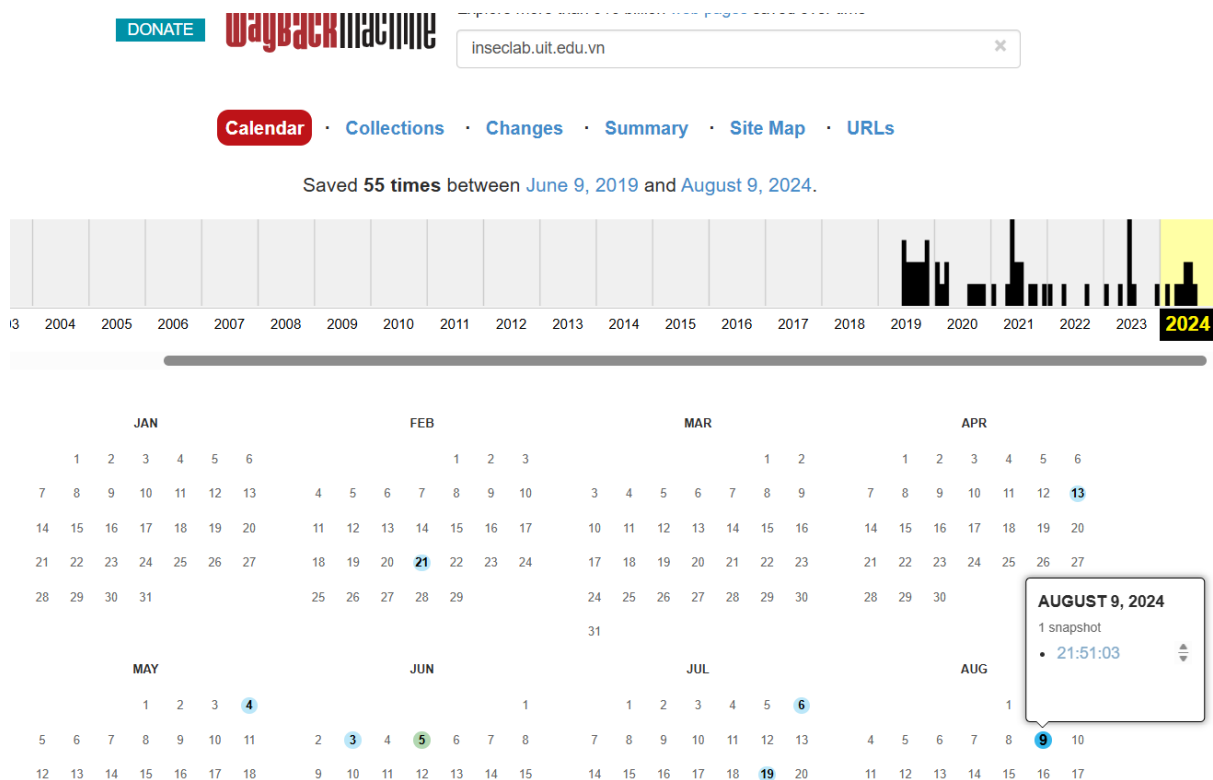
```

- Tìm kiếm các dữ liệu quá khứ của \*.uit.edu.vn

Dùng subdomainfinder để tìm các subdomain sau đó xem các thông tin tham khảo ở đây là last seen:

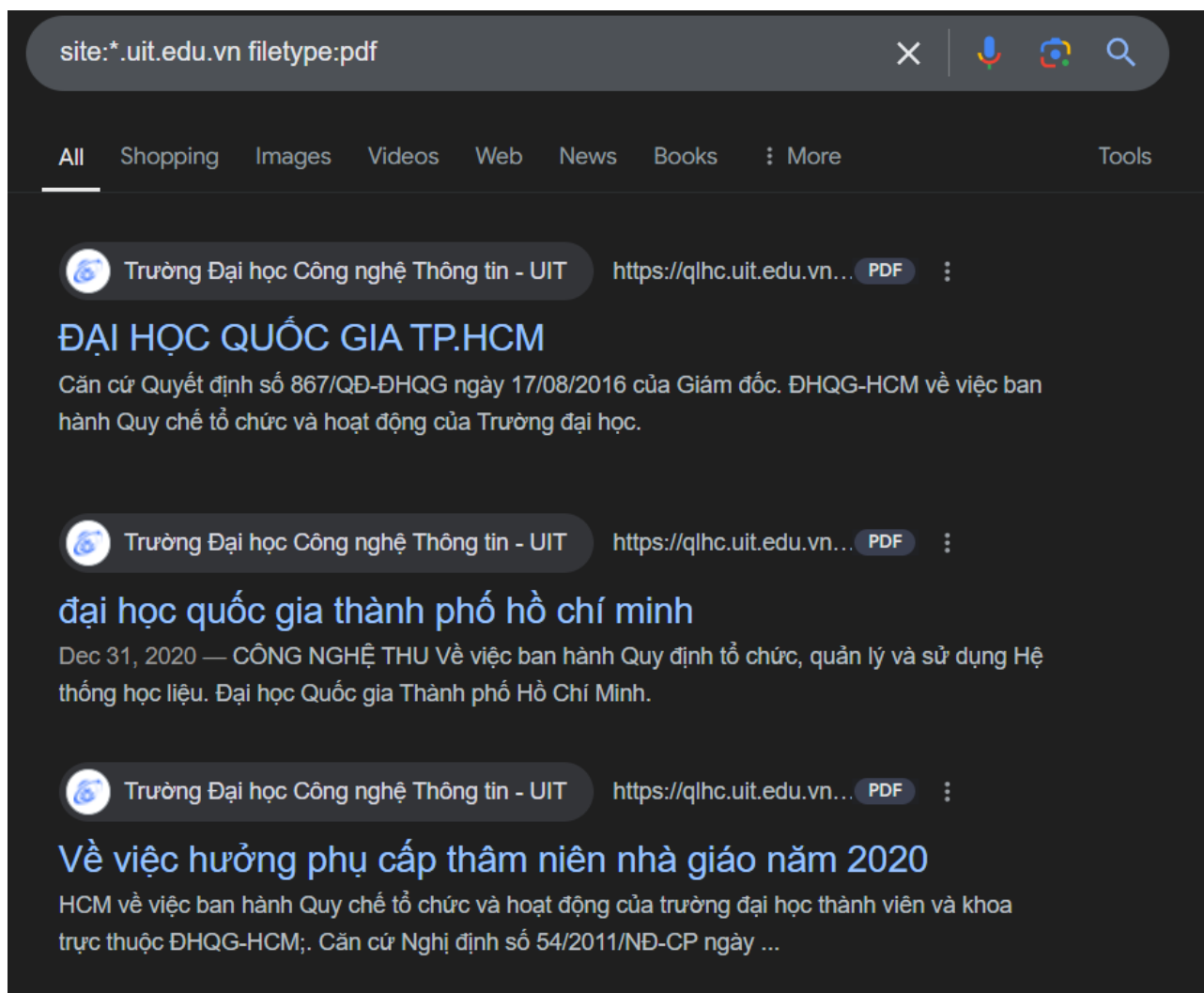
annotation.mmlab.uit.edu.vn	05-06-2024 08:10:19
api.mmlab.uit.edu.vn	12-06-2024 23:43:53
app.tech4covid.uit.edu.vn	21-09-2021 04:31:07
app1.iot.uit.edu.vn	21-10-2020 09:19:36
app2.iot.uit.edu.vn	21-10-2020 09:11:38
cbsv1.uit.edu.vn	10-07-2024 03:33:17
competitions.uit.edu.vn	07-02-2022 08:13:09
console-cloud.vlab.uit.edu.vn	11-07-2024 05:43:33
console-cloud.vlab2.uit.edu.vn	08-10-2022 15:42:43
cs.uit.edu.vn	25-10-2019 23:30:20
dsc.uit.edu.vn	15-07-2024 04:09:57
eth2.uit.edu.vn	07-04-2022 10:35:15
hcmccovidsafe-dev-gw.tech4covid.uit.edu.vn	10-10-2021 04:52:15
hcmccovidsafe-dev-gw2.tech4covid.uit.edu.vn	10-10-2021 04:52:15

Để kiểm dữ liệu trong quá khứ thì ta sẽ dùng trang web wayback machine.



- Tìm kiếm các dữ liệu nhạy cảm của \*.uit.edu.vn

Sử dụng filetype để đọc các tài liệu có thể chứa các thông tin chi tiết hơn của mục tiêu



Với các thông tin có thể thăm dò được có thể khai thác bằng tìm kiếm keyword đó

The screenshot shows a Google search interface with the search bar containing 'site:\*.uit.edu.vn "21521146"'. Below the search bar, there are tabs for 'All', 'Images', 'Shopping', 'Videos', 'News', 'Web', 'Books', 'More', and 'Tools'. The search results are displayed in a list format. The first result is from 'Trường Đại học Công nghệ Thông tin - UIT' with the URL 'https://ctsv.uit.edu.vn...' and a 'PDF' icon. The title is 'DANH SÁCH HỒ SƠ SINH VIÊN' and the snippet shows a list of student IDs and names: '571 21521146 Võ Sỹ Minh. Hoàn thành. Hoàn thành. Hoàn thành. 572 21521147 Hoàng Quý Mùi. Hoàn thành. Hoàn thành. Hoàn thành. 573 21521149 Lê Đoàn Trà My. Hoàn ...'. The second result is also from 'Trường Đại học Công nghệ Thông tin - UIT' with the URL 'https://ctsv.uit.edu.vn...' and an 'XLS' icon. The title is 'Sheet1' and the snippet shows a list of student IDs and names: '21521146, Võ Sỹ Minh, 7221701020, SV đăng ký ở KTX, chuyển tiền BHYT đã đóng qua học phí. 120, 115, 21521320, Đặng Hoàng Quân, 7523551386, 036 - Bệnh viện đa ...'. The third result is also from 'Trường Đại học Công nghệ Thông tin - UIT' with the URL 'https://ctsv.uit.edu.vn...' and an 'XLS' icon. The title is 'Sheet1' and the snippet shows a list of student IDs and names: '21521146, Võ Sỹ Minh, 7221701020, SV đăng ký ở KTX năm học 2021-2026. 15, 10, 21521894, Ma Văn Chương, 6623798165, SV đăng ký ở KTX năm học 2021-2027. 16, 11 ...'. The fourth result is also from 'Trường Đại học Công nghệ Thông tin - UIT' with the URL 'https://ctsv.uit.edu.vn...' and a 'PDF' icon. The title is 'DSSV MUA BHTN CHO SINH VIÊN NH 2021 04-10-2021 (1)'.

Có thể vào github để tìm kiếm sơ sót, lỗ hổng public của mục tiêu



374 files (2 s)

truongan/wecode-judge · setup.sh

```
52     if [ "$base_url" = "" ] ; then
53         base_url="https://khmt.uit.edu.vn/laptrinh/"echo $site_name | tr '[:upper:]' '[:lower:]'/"
54     fi
133 sed -i "s/homestead/$db_user/g" database.php
134 sed -i "s/$secret/$db_password/g" database.php
135 echo sed -i "s/sharif/$db/g" database.php
```

TxmMinh/run-devops · note.txt

```
120 Delete all info in file yml (service/deployment/replicaset/pod/secret/configmap)
137 - Get Kubernetes Secret:
138 kubectl get secret
190 - Create image pull Secret for ACR container:
191 kubectl create secret docker-registry acr-secret --docker-server=shoppingacr61524.azurecr.io --docker-username=shopping-
193 - Get Secret information in kubectl:
194 kubectl get secret
```

QuangDuong2903/Genesis · README.md

```
11
12 - Nguyen Cong Hoan - hoannc@uit.edu.vn
13
```

---

*Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này*

## YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, 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]-ExeX\_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).  
*Ví dụ: [NT101.K11.ANTT]-Exe01\_Group03.*
- 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 nộp.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

### Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

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

**HẾT**