

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA CÔNG NGHỆ THÔNG TIN 2

-----oOoOo-----



BÁO CÁO CUỐI KỲ

Môn học

Hệ Điều Hành Windows & Linux

Giảng viên : Đàm Minh Linh

Sinh viên thực hiện: Trần Quốc Trọng

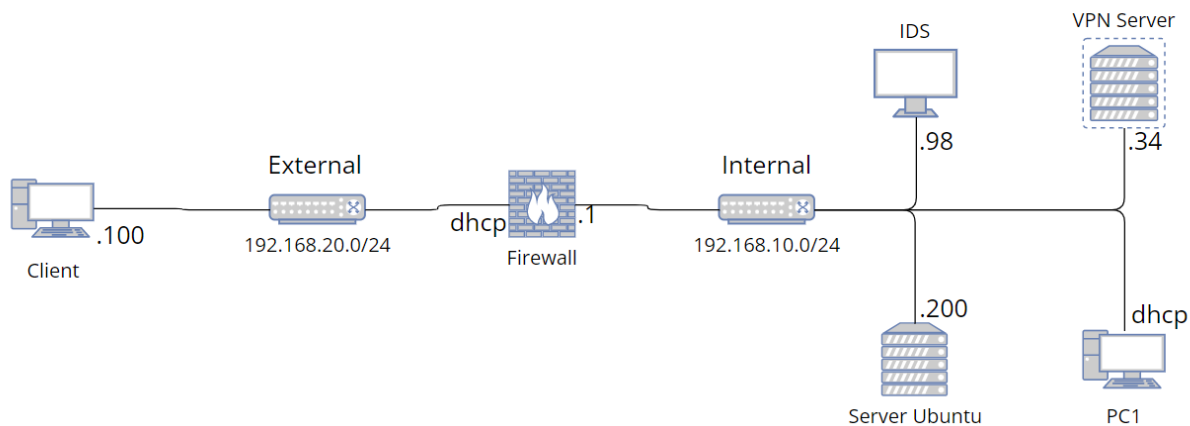
MSSV : N18DCAT100

TP.HCM, tháng 12/2022

MỤC LỤC

1. Sơ đồ mạng	1
2. Thực hiện	2
2.1. Quản lý user và group trên Ubuntu Server	2
2.1.1. Tạo users	2
2.1.2. Tạo Group và thêm users vào group	2
2.1.3. Phân quyền sở hữu và quyền truy cập tệp tin cho users	3
2.2. Cài đặt dịch vụ FTP trên Ubuntu Server	3
2.3. Cài đặt dịch vụ XRDP trên Ubuntu Server	5
2.4. Cài đặt dịch vụ VNC trên Ubuntu Server	6
2.5. Cài đặt dịch vụ SSH trên Ubuntu Server	8
2.6. Cài đặt dịch vụ DNS trên Ubuntu Server	9
2.7. Cài đặt dịch vụ DHCP trên Ubuntu Server	11
2.8. Cài đặt dịch vụ postfix gửi email trên Ubuntu Server	12
2.9. Triển khai IDS Nagios giám sát Ubuntu Server	14
2.9.1. Cài đặt và cấu hình IDS Nagios Server trên Ubuntu	14
2.9.2. Cài đặt NRPE giám sát Ubuntu Server	15
2.9.3. Thêm remote host trên Nagios Server (trên IDS)	16
2.9.4. Cài đặt Plugin nagios phát hiện tấn công DOS/DDOS web server	20
2.9.5. Cài đặt plugin nagios kiểm tra tên miền hết hạn	22
2.9.6. Cài đặt plugin nagios kiểm tra truy cập web online	24

1. Sơ đồ mạng



Tên thiết bị	Thông tin		Interface 1	Interface 2
Client	Windows 11 máy thật	Ip address		192.168.20.100
		Netmask		/24
		Default Gateway		
		DNS		
Firewall	Sophos UTM 9.6	Ip address	192.168.10.1	dhcp
		Netmask	/24	/24
		Default Gateway		
		DNS		
VPN Server	Windows Server 2019	Ip address	192.168.10.34	
		Netmask	/24	
		Default Gateway	192.168.10.1	
		DNS	192.168.10.34	
PC1	Windows 7	Ip address	dhcp	
		Netmask	/24	
		Default Gateway	192.168.10.1	
		DNS		
Server Ubuntu	Ubuntu 20.04 cài đặt các dịch vụ ftp, dhcp, dns, rdp, ssh, ...	Ip address	192.168.10.200	
		Netmask	/24	
		Default Gateway	192.168.10.1	
		DNS	8.8.8.8	
IDS	Ubuntu 20.04 cài Nagios	Ip address	192.168.10.98	
		Netmask	/24	
		Default Gateway	192.168.10.1	
		DNS	8.8.8.8	

2. Thực hiện

2.1. Quản lý user và group trên Ubuntu Server

2.1.1. Tạo users

- Tạo các user có tên: user1, user2, user3

```
$ sudo adduser user1  
$ sudo adduser user2  
$ sudo adduser user3
```

```
trg@trg-vm:~/Desktop$ sudo adduser user1  
[sudo] password for trg:  
Adding user `user1' ...  
Adding new group `user1' (1001) ...  
Adding new user `user1' (1001) with group `user1' ...  
Creating home directory `/home/user1' ...  
Copying files from `/etc/skel' ...  
New password:  
Retype new password:  
passwd: password updated successfully  
Changing the user information for user1  
Enter the new value, or press ENTER for the default  
    Full Name []:  
    Room Number []:  
    Work Phone []:  
    Home Phone []:  
    Other []:  
Is the information correct? [Y/n] y
```

2.1.2. Tạo Group và thêm users vào group

- Tạo các group users_basic, users_read_only

```
$ sudo groupadd users_basic  
$ sudo groupadd users_read_only
```

- Thêm user vào group

```
$ sudo usermod -g users_basic user1  
$ sudo usermod -g users_basic user2  
$ sudo usermod -g users_read_only user3
```

2.1.3. Phân quyền sở hữu và quyền truy cập tệp tin cho users

- Tạo thư mục dùng chung cho user1 và user2 có tên user_1_2

```
$ cd /home  
$ sudo mkdir user_1_2
```

```
trg@trg-vm:/home$ ls  
trg user1 user_1_2 user2 user3
```

- Thay đổi chủ sở hữu cho các thư mục

```
$ sudo chown -R user1:users_basic /home/user1  
$ sudo chown -R user2:users_basic /home/user2  
$ sudo chown -R user3:users_read_only /home/user3  
$ sudo chown -R :users_basic /home/user_1_2
```

```
trg@trg-vm:/home$ ls -l  
total 20  
drwxr-xr-x 19 trg trg 4096 Thg 11 24 21:51 trg  
drwxr-xr-x 2 user1 users_basic 4096 Thg 11 24 21:55 user1  
drwxr-xr-x 2 root users_basic 4096 Thg 11 24 22:11 user_1_2  
drwxr-xr-x 2 user2 users_basic 4096 Thg 11 24 21:56 user2  
drwxr-xr-x 2 user3 users_read_only 4096 Thg 11 24 21:56 user3
```

- Thay đổi quyền truy cập thư mục

```
$ sudo chmod 705 /home/user1  
$ sudo chmod 705 /home/user2  
$ sudo chmod 550 /home/user3  
$ sudo chmod 775 /home/user_1_2
```

```
trg@trg-vm:/home$ ls -l  
total 20  
drwxr-xr-x 19 trg trg 4096 Thg 11 24 21:51 trg  
drwx---r-x 2 user1 users_basic 4096 Thg 11 24 21:55 user1  
drwxrwxr-x 2 root users_basic 4096 Thg 11 24 22:11 user_1_2  
drwx---r-x 2 user2 users_basic 4096 Thg 11 24 21:56 user2  
dr-xr-x--- 2 user3 users_read_only 4096 Thg 11 24 21:56 user3
```

2.2. Cài đặt dịch vụ FTP trên Ubuntu Server

- Chạy các lệnh sau để cài đặt ftp service

```
$ sudo apt-get update  
$ sudo apt-get install vsftpd  
$ sudo service vsftpd status
```

```

trg@trg-vm:/home$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor prese>
   Active: active (running) since Thu 2022-11-24 22:49:19 +07; 2min 2s ago
   Main PID: 4177 (vsftpd)
     Tasks: 1 (limit: 4577)
    Memory: 524.0K
   CGroup: /system.slice/vsftpd.service
           └─4177 /usr/sbin/vsftpd /etc/vsftpd.conf

Thg 11 24 22:49:19 trg-vm systemd[1]: Starting vsftpd FTP server...
Thg 11 24 22:49:19 trg-vm systemd[1]: Started vsftpd FTP server.
lines 1-11/11 (END)

```

- Cấu hình ftp server

```

$ sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.bak
$ sudo nano /etc/vsftpd.conf

```

- Thêm hoặc bỏ comment các dòng sau vào file cấu hình

```

write_enable=YES
local_umask=022 #cung cấp cho các tệp và thư mục đã tải lên quyền chính xác.
force_dot_files=YES
allow_writeable_chroot=YES

```

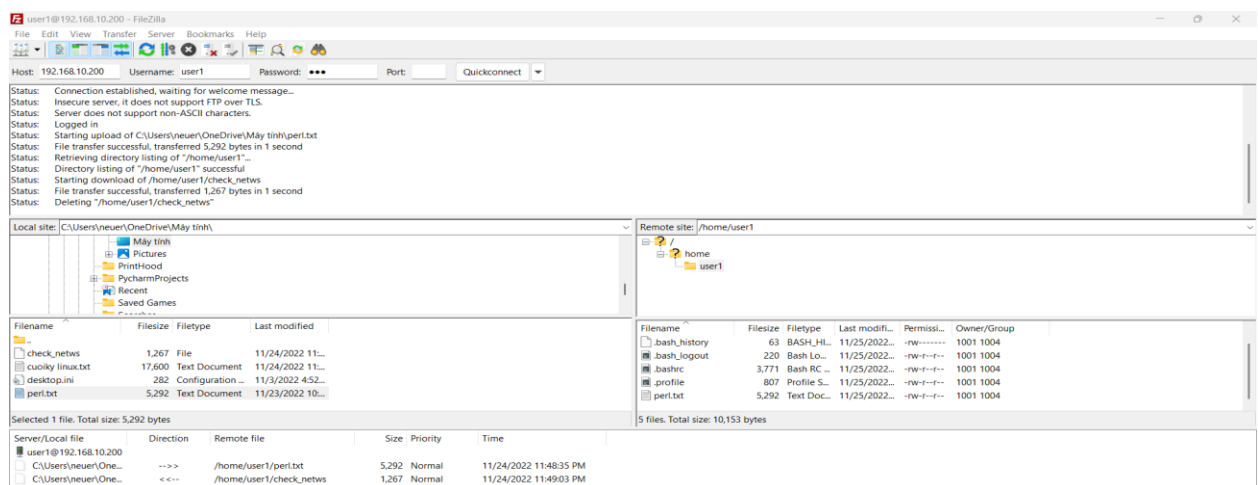
- Khởi động lại dịch vụ

```

$ sudo systemctl restart vsftpd

```

- Từ máy Client kết nối VPN và sử dụng FileZilla kiểm tra dịch vụ



2.3. Cài đặt dịch vụ XRDP trên Ubuntu Server

- Cài đặt XRDP

```
$ sudo apt update
$ sudo apt install xrdp -y
$ sudo systemctl status xrdp
```

```
trg@trg-vm:/home$ sudo systemctl status xrdp
● xrdp.service - xrdp daemon
   Loaded: loaded (/lib/systemd/system/xrdp.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-11-24 23:56:12 +07; 27s ago
     Docs: man:xrdp(8)
           man:xrdp.ini(5)
   Main PID: 4135 (xrdp)
      Tasks: 1 (limit: 4577)
    Memory: 752.0K
    CGroup: /system.slice/xrdp.service
            └─4135 /usr/sbin/xrdp

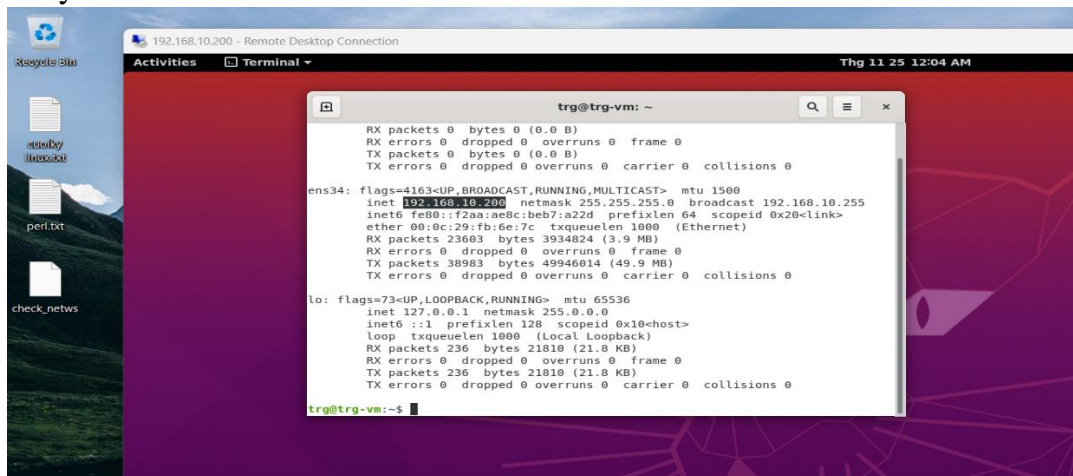
Thg 11 24 23:56:11 trg-vm xrdp[4134]: (4134)(140201039656768)[INFO ] address [0.0.0.0] port [3389] mode>
Thg 11 24 23:56:11 trg-vm xrdp[4134]: (4134)(140201039656768)[INFO ] listening to port 3389 on 0.0.0.0
Thg 11 24 23:56:11 trg-vm xrdp[4134]: (4134)(140201039656768)[INFO ] xrdp_listen_pp done
Thg 11 24 23:56:11 trg-vm xrdp[4134]: (4134)(140201039656768)[DEBUG] Closed socket 7 (AF_INET6 :: port >
```

- Cấu hình

```
$ sudo usermod -a -G ssl-cert xrdp
$ sudo gedit /etc/xrdp/startwm.sh
Thêm 2 dòng
unset DBUS_SESSION_BUS_ADDRESS
unset XDG_RUNTIME_DIR
$ sudo systemctl restart xrdp
```

```
29 if test -r /etc/profile; then
30     . /etc/profile
31 fi
32 unset DBUS_SESSION_BUS_ADDRESS
33 unset XDG_RUNTIME_DIR
34 test -x /etc/X11/Xsession && exec /etc/X11/Xsession
35 exec /bin/sh /etc/X11/Xsession
```

- Từ máy Client kết nối VPN và remote tới Ubuntu Server



2.4. Cài đặt dịch vụ VNC trên Ubuntu Server

- Cài đặt

```
$ sudo apt-get update
$ sudo apt-get install lightdm
$ sudo reboot
$ sudo apt-get install x11vnc
```

- Cấu hình

```
$ sudo nano /lib/systemd/system/x11vnc.service
Thêm các dòng sau:
-----
[Unit]
Description=x11vnc service
After=display-manager.service network.target syslog.target

[Service]
Type=simple
ExecStart=/usr/bin/x11vnc -forever -display :0 -auth guess -passwd password
ExecStop=/usr/bin/killall x11vnc
Restart=on-failure

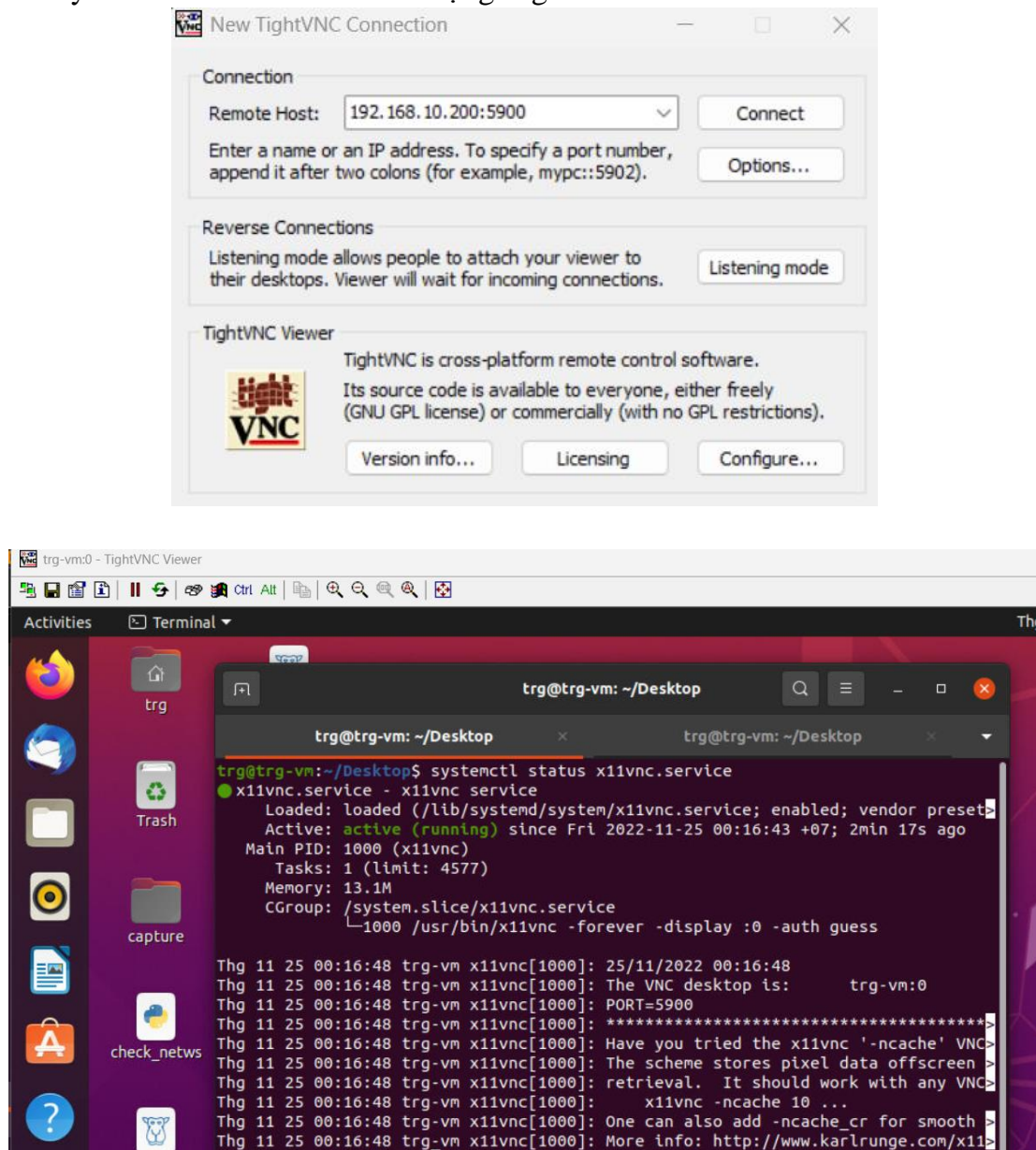
[Install]
WantedBy=multi-user.target
-----

Sau đó restart service
$ sudo systemctl daemon-reload
$ sudo systemctl enable x11vnc.service
$ sudo systemctl start x11vnc.service
$ sudo systemctl status x11vnc.service
```

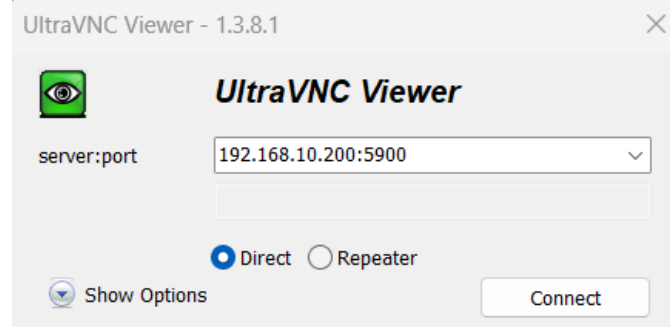
```
trg@trg-vm:~/Desktop$ systemctl status x11vnc.service
● x11vnc.service - x11vnc service
   Loaded: loaded (/lib/systemd/system/x11vnc.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2022-11-25 00:16:43 +07; 2min 17s ago
     Main PID: 1000 (x11vnc)
        Tasks: 1 (limit: 4577)
       Memory: 13.1M
      CGroup: /system.slice/x11vnc.service
              └─1000 /usr/bin/x11vnc -forever -display :0 -auth guess

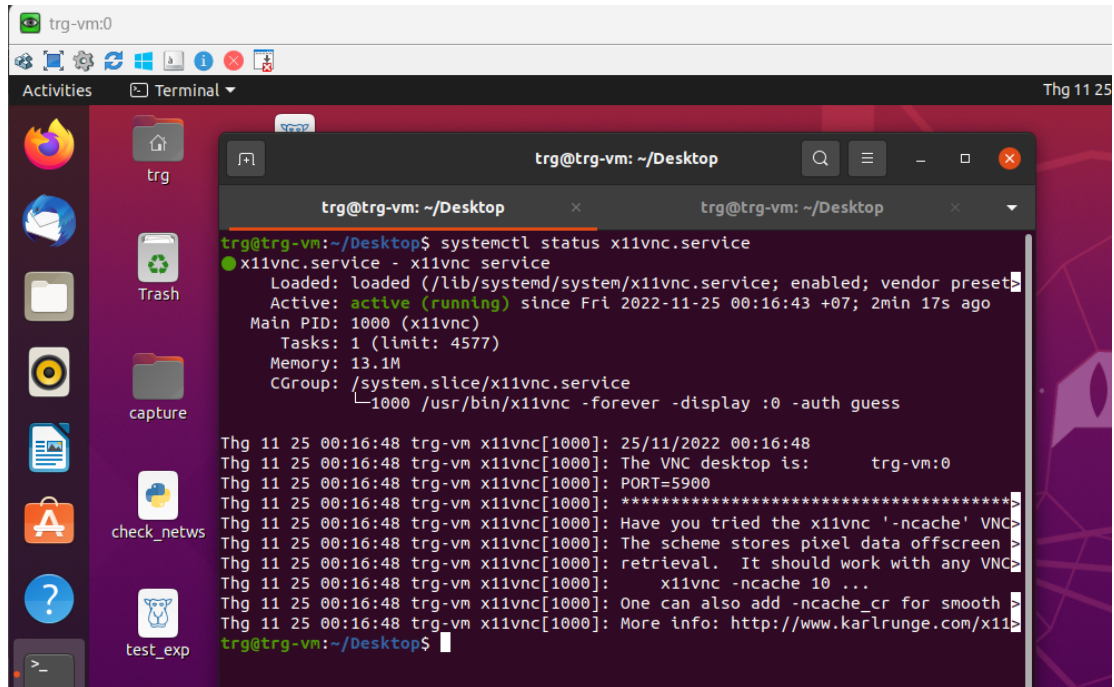
Thg 11 25 00:16:48 trg-vm x11vnc[1000]: 25/11/2022 00:16:48
Thg 11 25 00:16:48 trg-vm x11vnc[1000]: The VNC desktop is:      trg-vm:0
Thg 11 25 00:16:48 trg-vm x11vnc[1000]: PORT=5900
Thg 11 25 00:16:48 trg-vm x11vnc[1000]: *****
Thg 11 25 00:16:48 trg-vm x11vnc[1000]: Have you tried the x11vnc '-ncache' VNC
Thg 11 25 00:16:48 trg-vm x11vnc[1000]: The scheme stores pixel data offscreen
Thg 11 25 00:16:48 trg-vm x11vnc[1000]: retrieval. It should work with any VNC
Thg 11 25 00:16:48 trg-vm x11vnc[1000]: x11vnc -ncache 10 ...
Thg 11 25 00:16:48 trg-vm x11vnc[1000]: One can also add -ncache_cr for smooth
Thg 11 25 00:16:48 trg-vm x11vnc[1000]: More info: http://www.karlrunge.com/x11vnc/
```


- Từ máy Client kết nối VPN và sử dụng TightVNC Viewer remote Ubuntu Server



- Từ máy Client kết nối VPN và sử dụng UltraVNC Viewer remote Ubuntu Server





2.5. Cài đặt dịch vụ SSH trên Ubuntu Server

- Cài đặt

```

$ sudo apt install openssh-server
$ sudo systemctl status sshd

```

```

trg@trg-vm:~/Desktop$ sudo systemctl status sshd
[sudo] password for trg:
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2022-11-25 00:16:42 +07; 20min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 849 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 900 (sshd)
         Tasks: 1 (limit: 4577)
        Memory: 2.2M
       CGroup: /system.slice/ssh.service
               └─900 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Thg 11 25 00:16:41 trg-vm systemd[1]: Starting OpenBSD Secure Shell server...
Thg 11 25 00:16:42 trg-vm systemd[1]: Started OpenBSD Secure Shell server.
Thg 11 25 00:16:42 trg-vm sshd[900]: Server listening on 0.0.0.0 port 22.
Thg 11 25 00:16:42 trg-vm sshd[900]: Server listening on :: port 22.

```

- Từ máy Client kết nối VPN và thực hiện kết nối putty ssh tới Ubuntu Server

```

trg@trg-vm: ~
login as: trg
trg@192.168.10.200's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.15.0-53-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

31 updates can be applied immediately.
7 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Fri Nov 18 20:22:13 2022 from 192.168.20.100
trg@trg-vm:~$

```

2.6. Cài đặt dịch vụ DNS trên Ubuntu Server

- Cài đặt

```
$ sudo apt-get update
$ sudo apt-get install bind9 bind9utils
```

- Cấu hình

```
$ sudo gedit /etc/bind/named.conf.local
```

Thêm các dòng sau:

```
-----
zone "tranquoctruong.com" IN { // Domain name
    type master; // Primary DNS
    file "/etc/bind/tranquoctruong.com.db"; // Forward Zone file
};
```

```
zone "10.168.192.in-addr.arpa" IN { // Reverse lookup name
    type master; // Primary DNS
    file "/etc/bind/r.tranquoctruong.com.db"; // Reverse lookup file
};
-----
```

```
$ cp /etc/bind/db.local /etc/bind/tranquoctruong.com.db
$ cp /etc/bind/db.127 /etc/bind/r.tranquoctruong.com.db
```

```
$ sudo gedit /etc/bind/tranquoctruong.com.db
```

Thêm các dòng sau:

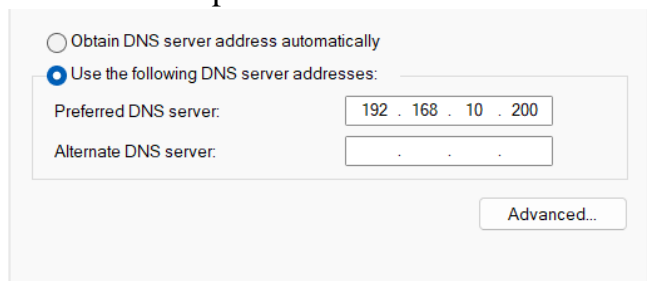
```
-----
; BIND data file for local loopback interface
;
$TTL 604800
@      IN      SOA  ns.tranquoctruong.com. root.tranquoctruong.com. (
                                2          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@      IN      NS   ns.tranquoctruong.com.
@      IN      A    192.168.10.200
ns     IN      A    192.168.10.200
www    IN      CNAME ns
-----
```

```
$ sudo gedit /etc/bind/r.tranquoctruong.com.db
```

Thêm các dòng sau

```
-----  
; BIND reverse data file for local loopback interface  
;  
$TTL 604800  
@      IN      SOA  ns.tranquoctruong.com. root.tranquoctruong.com. (  
                                1          ; Serial  
                                604800     ; Refresh  
                                86400      ; Retry  
                                2419200    ; Expire  
                                604800 )   ; Negative Cache TTL  
;  
@      IN      NS   ns.tranquoctruong.com.  
200    IN      PTR  ns.tranquoctruong.com.  
-----  
$ sudo systemctl restart bind9.service
```

- Đặt lại DNS server cho kết nối vpn



- Từ máy Client kết nối VPN và thực hiện truy vấn phân giải tên miền

```
C:\Users\neuer>nslookup  
Default Server:  ns.tranquoctruong.com  
Address:  192.168.10.200  
  
> tranquoctruong.com  
Server:  ns.tranquoctruong.com  
Address:  192.168.10.200  
  
Name:    tranquoctruong.com  
Address:  192.168.10.200  
  
> 192.168.10.200  
Server:  ns.tranquoctruong.com  
Address:  192.168.10.200  
  
Name:    ns.tranquoctruong.com  
Address:  192.168.10.200  
  
> |
```

2.7. Cài đặt dịch vụ DHCP trên Ubuntu Server

- Cài đặt

```
$ sudo apt install isc-dhcp-server -y
$ sudo systemctl start isc-dhcp-server
$ sudo systemctl enable isc-dhcp-server
```

- Cấu hình

```
$ sudo gedit /etc/default/isc-dhcp-server
Thêm 2 dòng sau
INTERFACESv4="ens34"
INTERFACESv6=""

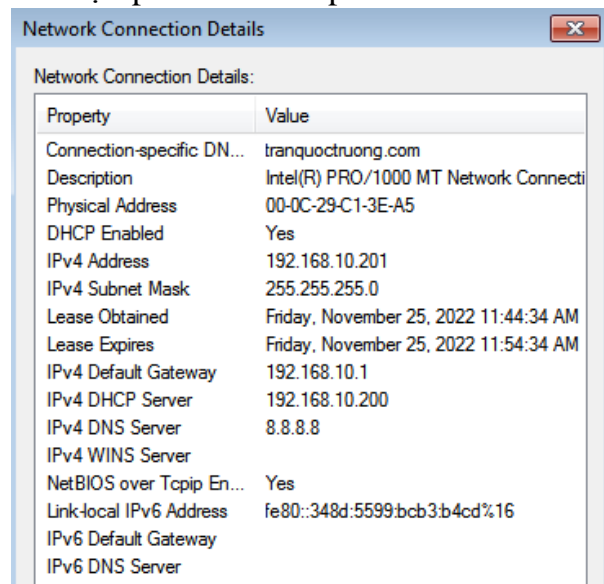
$ sudo gedit /etc/dhcp/dhcpd.conf
Bỏ comment các dòng sau
subnet 192.168.10.0 netmask 255.255.255.0 {
    range 192.168.10.100 192.168.10.254;
    option domain-name-servers ns.tranquoctruong.com, 8.8.8.8;
    option domain-name "tranquoctruong.com";
    option subnet-mask 255.255.255.0;
    option routers 192.168.10.1;
    option broadcast-address 192.168.10.255;
    default-lease-time 600;
    max-lease-time 7200;
}

$ sudo systemctl restart isc-dhcp-server
$ sudo systemctl status isc-dhcp-server
```

```
trg@trg-vm:~/Desktop$ sudo systemctl status isc-dhcp-server
[sudo] password for trg:
● isc-dhcp-server.service - ISC DHCP IPv4 server
   Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2022-11-25 00:16:50 +07; 11h ago
     Docs: man:dhcpd(8)
    Main PID: 1380 (dhcpd)
      Tasks: 4 (limit: 4577)
    Memory: 6.5M
    CGroup: /system.slice/isc-dhcp-server.service
            └─1380 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dh

Thg 11 25 00:16:50 trg-vm dhcpd[1380]: PID file: /run/dhcp-server/dhcpd.pid
Thg 11 25 00:16:50 trg-vm dhcpd[1380]: Wrote 1 leases to leases file.
Thg 11 25 00:16:50 trg-vm sh[1380]: Wrote 1 leases to leases file.
Thg 11 25 00:16:50 trg-vm sh[1380]: Listening on LPF/ens34/00:0c:29:fb:6e:7c/192.168.10.0
Thg 11 25 00:16:50 trg-vm sh[1380]: Sending on LPF/ens34/00:0c:29:fb:6e:7c/192.168.10.0
Thg 11 25 00:16:50 trg-vm sh[1380]: Sending on Socket/fallback/fallback-net
Thg 11 25 00:16:50 trg-vm dhcpd[1380]: Listening on LPF/ens34/00:0c:29:fb:6e:7c/192.168.10.0
Thg 11 25 00:16:50 trg-vm dhcpd[1380]: Sending on LPF/ens34/00:0c:29:fb:6e:7c/192.168.10.0
Thg 11 25 00:16:50 trg-vm dhcpd[1380]: Sending on Socket/fallback/fallback-net
Thg 11 25 00:16:50 trg-vm dhcpd[1380]: Server starting service.
```

- Từ máy Windows 7 cài đặt ipv4 thành dhcp



- Kiểm tra lại ip đã cấp phát trên Ubuntu Server

```
trg@trg-vm:~/Desktop$ dhcpd-lease-list
To get manufacturer names please download http://standards.ieee.org/regauth/oui/oui.txt to /usr/local/etc/oui.txt
Reading leases from /var/lib/dhcp/dhcpd.leases
=====
MAC                IP                hostname          valid until       manufacturer
=====
00:0c:29:c1:3e:a5  192.168.10.201   trg-PC            2022-11-25 04:54:35 -NA-
```

2.8. Cài đặt dịch vụ postfix gửi email trên Ubuntu Server

- Cài đặt

```
$ sudo apt-get install libsasl2-modules postfix
```

- Tạo mật khẩu ứng dụng trên gmail tại <https://myaccount.google.com/security>
- Cấu hình

```
$ sudo gedit /etc/postfix/sasl/sasl_passwd
Thêm dòng sau
[smtplib@gmail.com]:587 <tài khoản>@gmail.com:<mật khẩu>

$ sudo postmap /etc/postfix/sasl/sasl_passwd
$ sudo chown root:root /etc/postfix/sasl/sasl_passwd /etc/postfix/sasl/sasl_passwd.db
$ sudo chmod 0600 /etc/postfix/sasl/sasl_passwd /etc/postfix/sasl/sasl_passwd.db

$ sudo gedit /etc/postfix/main.cf
Thay thế dòng relayhost và thêm các dòng sau vào cuối file
relayhost = [smtplib@gmail.com]:587

# Enable SASL authentication
smtp_sasl_auth_enable = yes
```

```
# Disallow methods that allow anonymous authentication
smtp_sasl_security_options = noanonymous
# Location of sasl_passwd
smtp_sasl_password_maps = hash:/etc/postfix/sasl/sasl_passwd
# Enable STARTTLS encryption
smtp_tls_security_level = encrypt
# Location of CA certificates
smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt
```

Khởi động lại dịch vụ

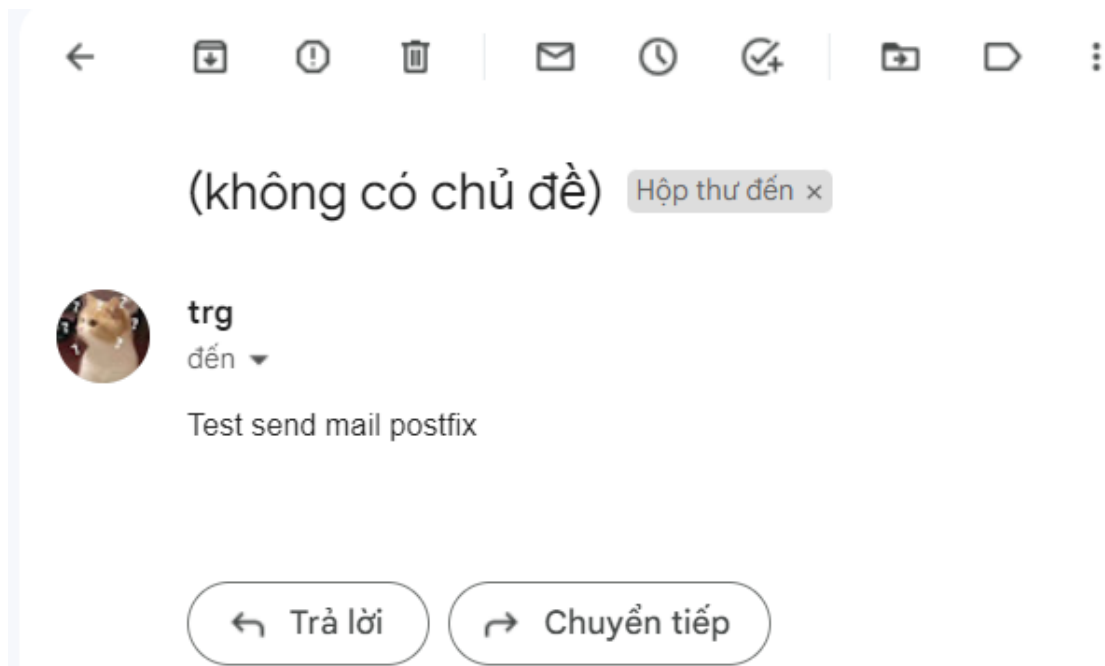
```
$ sudo systemctl restart postfix
```

```
$ sudo systemctl enable postfix
```

```
$ sudo systemctl status postfix
```

- Thực hiện gửi email kiểm tra

```
trg@trg-vm:~/Desktop$ sendmail trantruongac1@gmail.com
sendmail: warning: /etc/postfix/main.cf, line 57: overriding earlier entry: smtp_tls_security_level=may
postdrop: warning: /etc/postfix/main.cf, line 57: overriding earlier entry: smtp_tls_security_level=may
Test send mail postfix
.
```



2.9. Triển khai IDS Nagios giám sát Ubuntu Server

2.9.1. Cài đặt và cấu hình IDS Nagios Server trên Ubuntu

- Cài đặt

```
$ sudo apt update
$ sudo apt install apache2
$ sudo a2enmod authz_groupfile auth_digest
$ sudo apt install nagios4 nagios-nrpe-plugin nagios-plugins-contrib
$ sudo htdigest -c /etc/nagios4/htdigest.users Nagios4 nagiosadmin
```

- Cấu hình

```
$ sudo gedit /etc/apache2/conf-enabled/nagios4-cgi.conf
```

```
34 #
35 # Require ip          :::1/128 fc00::/7 fe80::/10 10.0.0.0/8
36 # <Files "cmd.cgi">
37     AuthDigestDomain "Nagios4"
38     AuthDigestProvider file
39     AuthUserFile      "/etc/nagios4/htdigest.users"
40     AuthGroupFile     "/etc/group"
41     AuthName          "Nagios4"
42     AuthType          Digest
43 # Require all        granted
44     Require          valid-user
45 # </Files>
46 </DirectoryMatch>
47
48 <Directory /usr/share/nagios4/htdocs>
49     Options          +ExecCGI
50 </Directory>
```

```
$ sudo gedit /etc/nagios4/cgi.cfg
```

use_authentication=1

- Cài đặt postfix (các bước như ở phần trước)
- Kiểm tra lại file command.cfg

```
$ sudo gedit /etc/nagios4/objects/commands.cfg
```

```
26 # 'notify-host-by-email' command definition
27 define command{
28     command_name    notify-host-by-email
29     command_line     /usr/bin/printf "%b" "***** Nagios *****\nNotification Type: $NOTIFICATIONTYPE$\nHost: $HOSTNAME$\nState: $HOSTSTATE$\nAddress: $HOSTADDRESS$\nInfo: $HOSTOUTPUT$\n\nDate/Time: $LONGDATETIME$\n" | /usr/bin/mail -s "*** $NOTIFICATIONTYPE$ Host Alert: $HOSTNAME$ is $HOSTSTATE$ ***" $CONTACTEMAIL$
30 }
31
32 # 'notify-service-by-email' command definition
33 define command{
34     command_name    notify-service-by-email
35     command_line     /usr/bin/printf "%b" "***** Nagios *****\nNotification Type: $NOTIFICATIONTYPE$\nService: $SERVICEDESC$\nHost: $HOSTALIAS$\nAddress: $HOSTADDRESS$\nState: $SERVICESTATE$\n\nDate/Time: $LONGDATETIME$\n\nAdditional Info: $SERVICEOUTPUT$\n" | /usr/bin/mail -s "*** $NOTIFICATIONTYPE$ Service Alert: $HOSTALIAS$/$SERVICEDESC$ is $SERVICESTATE$ ***" $CONTACTEMAIL$
36 }
```

- Thêm địa chỉ email muốn nhận thông báo từ nagios


```

$ sudo gedit /etc/nagios4/objects/contacts.cfg
28
29 define contact{
30     contact_name      nagiosadmin          ; Short name of user
31     use                generic-contact      ; Inherit default values from generic-contact template
32     alias              Nagios Admin         ; Full name of user
33
34     email              trantruongac1@gmail.com ; <<***** CHANGE THIS TO YOUR EMAIL ADDRESS *****>>
35 }
36

```

- Kiểm tra “contact_groups admins” có trong generic-service, generic-host

```
$ sudo cat /etc/nagios4/objects/templates.cfg
```

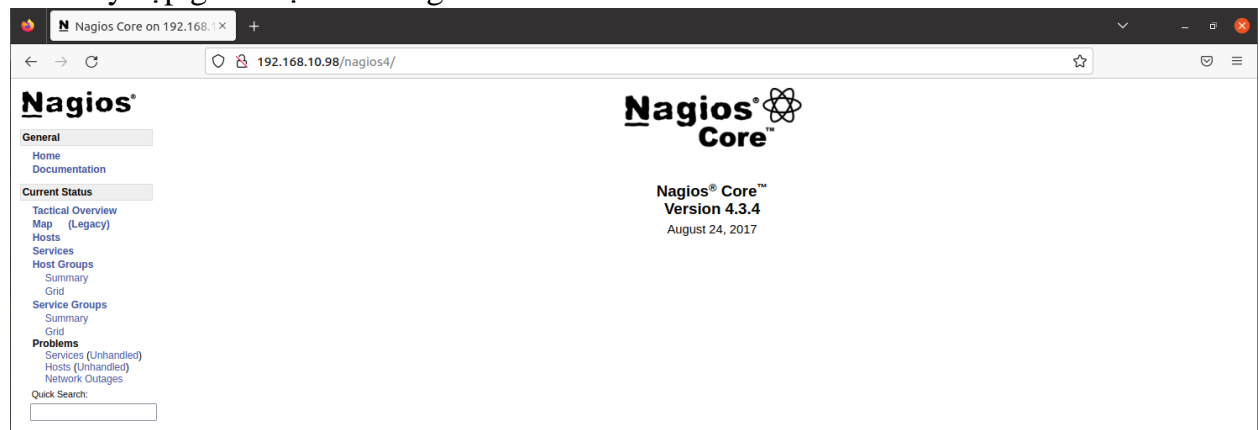
- Khởi động lại dịch vụ

```

$ sudo systemctl restart apache2
$ sudo systemctl restart nagios4

```

- Truy cập giao diện web nagios



2.9.2. Cài đặt NRPE giám sát Ubuntu Server

- Trên máy Ubuntu Server chạy các lệnh sau

```

$ sudo apt update
$ sudo apt install nagios-nrpe-server nagios-plugins

```

- Cấu hình

```

$ sudo gedit /etc/nagios/nrpe.cfg

```

Chỉnh sửa các dòng sau:

```

server_address=<ip-host>
allowed_hosts=127.0.0.1,::1, <ip-server>

```

```

$ sudo gedit /etc/nagios/nrpe_local.cfg

```

Thêm các command sau:

```

command[check_root]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /
command[check_ping]=/usr/lib/nagios/plugins/check_ping -H 192.168.10.200 -w
100.0,20% -c 500.0,60% -p 5
command[check_ssh]=/usr/lib/nagios/plugins/check_ssh -4 192.168.10.200
command[check_http]=/usr/lib/nagios/plugins/check_http -I google.com
command[check_apt]=/usr/lib/nagios/plugins/check_apt
command[check_users]=/usr/lib/nagios/plugins/check_users -w 5 -c 10
command[check_load]=/usr/lib/nagios/plugins/check_load -w 15,10,5 -c 30,25,20
command[check_hda1]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /home/trg
command[check_zombie_procs]=/usr/lib/nagios/plugins/check_procs -w 5 -c 10 -s Z
command[check_total_procs]=/usr/lib/nagios/plugins/check_procs -w 150 -c 200

```

Sau đó restart lại server

```
$ sudo systemctl restart nagios-nrpe-server
```

2.9.3. Thêm remote host trên Nagios Server (trên IDS)

- Trên Nagios Server thực hiện các lệnh sau:

```

$ sudo gedit /etc/nagios4/nagios.cfg
Bỏ comment dòng: "cfg_dir=/usr/local/nagios/etc/servers"

$ cd /etc/nagios4/
$ sudo mkdir servers
$ cd servers/
$ sudo gedit /etc/nagios4/servers/nagiosclient.cfg
Thêm các dòng sau:
define host {
    use                linux-server
    host_name          trg-vm
    alias              Ubuntu Host
    address            192.168.10.200
    register           1
}

define service {
    host_name          trg-vm
    service_description PING
    check_command      check_nrpe!check_ping
    max_check_attempts 2
    check_interval     2
    retry_interval     2
    check_period       24x7
}

```

```

    check_freshness          1
    contact_groups            admins
    notification_interval     2
    notification_period       24x7
    notifications_enabled     1
    register                  1
}

define service {
    host_name                trg-vm
    service_description      Check Users
    check_command             check_nrpe!check_users
    max_check_attempts       2
    check_interval           2
    retry_interval           2
    check_period              24x7
    check_freshness          1
    contact_groups            admins
    notification_interval     2
    notification_period       24x7
    notifications_enabled     1
    register                  1
}

define service {
    host_name                trg-vm
    service_description      Check SSH
    check_command             check_nrpe!check_ssh
    max_check_attempts       2
    check_interval           2
    retry_interval           2
    check_period              24x7
    check_freshness          1
    contact_groups            admins
    notification_interval     2
    notification_period       24x7
    notifications_enabled     1
    register                  1
}

define service {
    host_name                trg-vm
    service_description      Check Root / Disk

```

```

check_command          check_nrpe!check_root
max_check_attempts     2
check_interval         2
retry_interval         2
check_period           24x7
check_freshness        1
contact_groups         admins
notification_interval   2
notification_period     24x7
notifications_enabled   1
register               1
}

define service {
    host_name            trg-vm
    service_description   Check APT Update
    check_command         check_nrpe!check_apt
    max_check_attempts    2
    check_interval        2
    retry_interval        2
    check_period          24x7
    check_freshness       1
    contact_groups        admins
    notification_interval  2
    notification_period    24x7
    notifications_enabled  1
    register              1
}

define service {
    host_name            trg-vm
    service_description   Check HTTP
    check_command         check_nrpe!check_http
    max_check_attempts    2
    check_interval        2
    retry_interval        2
    check_period          24x7
    check_freshness       1
    contact_groups        admins
    notification_interval  2
    notification_period    24x7
    notifications_enabled  1
    register              1
}

```

```

}

define service {
    host_name            trg-vm
    service_description   check trg Disk
    check_command         check_nrpe!check_hda1
    max_check_attempts    2
    check_interval        2
    retry_interval        2
    check_period          24x7
    check_freshness       1
    contact_groups        admins
    notification_interval 2
    notification_period    24x7
    notifications_enabled  1
    register              1
}

define service {
    host_name            trg-vm
    service_description   Total Processes
    check_command         check_nrpe!check_total_procs
    max_check_attempts    2
    check_interval        2
    retry_interval        2
    check_period          24x7
    check_freshness       1
    contact_groups        admins
    notification_interval 2
    notification_period    24x7
    notifications_enabled  1
    register              1
}

define service {
    host_name            trg-vm
    service_description   Current Load
    check_command         check_nrpe!check_load
    max_check_attempts    2
    check_interval        2
    retry_interval        2
    check_period          24x7
    check_freshness       1

```

```

contact_groups      admins
notification_interval 2
notification_period 24x7
notifications_enabled 1
register            1
}

```

Sau đó lưu lại file và khởi động lại nagios:

```
$ sudo systemctl restart nagios4.service
```

- Truy cập giao diện web và kiểm tra

- Nagios gửi email thông báo

2.9.4. Cài đặt Plugin nagios phát hiện tấn công DOS/DDOS web server

- Chức năng của plugin: đếm số lượng các ip đang giao tiếp với Ubuntu Server
- Cài đặt gói cần thiết trên Ubuntu Server:

```

$ sudo apt update -y
$ sudo apt install wireshark
$ sudo apt install python3-pip
$ sudo pip3 install pyshark
$ sudo apt install tshark

```

```
$ mkdir /home/trg/Desktop
$ sudo chmod -R 777 /home/trg/Desktop
```

- Tạo script python

```
$ sudo gedit /usr/lib/nagios/plugins/check_netws
$ sudo chmod a+x /usr/lib/nagios/plugins/check_netws
```

```
1#!/usr/bin/python3
2import pyshark
3import sys
4
5path_pcap_file = r'/home/trg/Desktop/capture/m.pcap'
6ip_server = '192.168.10.200'
7port_server = '80' # http port
8iface_name = 'ens34'
9display_filter_string = 'tcp.flags.syn==1 && tcp.flags.ack==0 && tcp.dstport=={} && ip.dst=={}'.format(port_server, ip_server)
10connection_risk = {} # {"ip-client": "number syn packet"}
11
12def check_dos(packet):
13    global connection_risk
14    source_ip = ''
15    if 'ip' in packet and 'src' in packet.ip.field_names:
16        source_ip = str(packet.ip.src)
17    if source_ip != '':
18        if source_ip not in connection_risk:
19            connection_risk[source_ip] = 1
20        else:
21            connection_risk[source_ip] += 1
22
23    if sum(connection_risk.values()) >= 70:
24        return True
25    return False
26
27
28if __name__ == '__main__':
29    try:
30        packets = pyshark.LiveCapture(iface_name, output_file=path_pcap_file)
31        packets.sniff(timeout=10)
32        packets.close()
33        packets = pyshark.FileCapture(path_pcap_file, display_filter=display_filter_string)
34        for packet in packets:
35            if check_dos(packet):
36                break
37    except:
38        print('error when capture packets')
39        sys.exit(3)
40
41    if sum(connection_risk.values()) >= 70 and len(connection_risk) >= 40:
42        print('CRITICAL - Possible DDoS Attack Type SYN flood!')
43        sys.exit(2)
44
45    elif sum(connection_risk.values()) >= 60 and len(connection_risk) >= 36:
46        print('WARNING - Possible DDoS Attack Type SYN flood!')
47        sys.exit(1)
48
49    for ip in connection_risk:
50        if connection_risk[ip] >= 70:
51            print('CRITICAL - Possible DoS Attack Type SYN flood from {}'.format(ip))
52            sys.exit(2)
53        elif connection_risk[ip] >= 60:
54            print('WARNING - Possible DoS Attack Type SYN flood from {}'.format(ip))
55            sys.exit(1)
56
57    print('OK - No abnormality detected')
58    sys.exit(0)
```

- Cấu hình trên Ubuntu Server

```
$ sudo gedit /etc/nagios/nrpe_local.cfg
Thêm dòng sau:
command[check_netws]=sudo /usr/lib/nagios/plugins/check_netws
```

Để nagios có thể thực hiện command với quyền sudo không cần mật khẩu thêm dòng sau:

```
$ sudo gedit /etc/sudoers
nagios ALL=(ALL) NOPASSWD:/usr/lib/nagios/plugins/check_netws
```

- Khởi động lại nrpe

```
$ sudo systemctl restart nagios-nrpe-server
```

- Trên Nagios Server thêm service

```
$ sudo gedit /etc/nagios4/servers/nagiosclient.cfg
Thêm dòng sau:
define service {
    host_name                trg-vm
    service_description      Check net pyshark
    check_command             check_nrpe!check_netws -t 30
    max_check_attempts       2
    check_interval            2
    retry_interval            2
    check_period              24x7
    check_freshness           1
    contact_groups            admins
    notification_interval     2
    notification_period       24x7
    notifications_enabled     1
    register                  1
}
```

- Khởi động lại nagios server

```
$ sudo systemctl restart nagios4.service
```

2.9.5. Cài đặt plugin nagios kiểm tra tên miền hết hạn

- Trên máy Ubuntu Server cài đặt các gói cần thiết

```
$ sudo apt update -y
$ sudo apt install whois
$ sudo apt-get install -y libdatetime-perl
$ sudo apt-get install -y libdatetime-format-iso8601-perl
$ sudo apt-get install -y libjson-perl
```


- Tạo script perl

```
$ sudo gedit /usr/lib/nagios/plugins/check_domain_exp
$ sudo chmod a+x /usr/lib/nagios/plugins/check_domain_exp
1#!/usr/bin/perl
2|
3use strict;
4use warnings;
5use DateTime;
6use DateTime::Format::ISO8601;
7use LWP::Simple qw(get);
8use JSON      qw(decode_json);
9
10my $domainName = shift or do{
11    print "Usage: $0 DOMAIN_NAME\n";
12    exit 3;
13};
14
15my $exp_date = `whois $domainName | grep "Expiration Date" | rev | cut -d' ' -f1 | rev`;
16unless($exp_date){
17    my $url_api = 'https://whois.inet.vn/api/whois/domainspecify/'.$domainName;
18    my $json = decode_json(get($url_api));
19    my $expirationDate = $json->{expirationDate};
20    unless($expirationDate){
21        print "UNKNOWN - domain \"$domainName\" not found expiration date\n";
22        exit 3;
23    }
24    my ($day, $month, $year) = split(/-/, $expirationDate);
25    $exp_date = DateTime->new(
26        year      => int($year),
27        month     => int($month),
28        day       => int($day),
29    );
30} else {
31    $exp_date = DateTime::Format::ISO8601->parse_datetime( $exp_date );
32}
33
34my $current_date = DateTime->now(time_zone => 'Asia/Ho_Chi_Minh');
35if($exp_date > $current_date){
36    my $days = int($exp_date->delta_days($current_date)->delta_days());
37    if($days > 0 and $days <= 7){
38        print "CRITICAL - \"$domainName\" $days days left to expire.\n";
39        exit 2;
40    }
41    elsif($days > 7 and $days <= 30){
42        print "WARNING - \"$domainName\" $days days left to expire.\n";
43        exit 1;
44    }
45    elsif($days > 30){
46        print "OK - \"$domainName\" $days days left to expire.\n";
47        exit 0;
48    }
49}
50elsif($exp_date <= $current_date){
51    print "CRITICAL - \"$domainName\" has expired.\n";
52    exit 2;
53}
```

- Cấu hình trên Ubuntu Server

```
$ sudo gedit /etc/nagios/nrpe_local.cfg
Thêm dòng sau:
command[check_domain_exp]=/usr/lib/nagios/plugins/check_domain_exp
google.com
```

- Khởi động lại nrpe

```
$ sudo systemctl restart nagios-nrpe-server
```

- Trên Nagios Server thêm service

```
$ sudo gedit /etc/nagios4/servers/nagiosclient.cfg
Thêm dòng sau:
define service {
    host_name                trg-vm
    service_description      Check domain expiration date
    check_command             check_nrpe!check_domain_exp -t 30
    max_check_attempts       2
    check_interval            0.1
    retry_interval            0.1
    check_period              24x7
    check_freshness           1
    contact_groups            admins
    notification_interval     2
    notification_period       24x7
    notifications_enabled     1
    register                  1
}
```

- Khởi động lại nagios server

```
$ sudo systemctl restart nagios4.service
```

2.9.6. Cài đặt plugin nagios kiểm tra truy cập web online

- Cài đặt apache2

```
$ sudo apt install apache2
```

- Tạo script perl

```
$ sudo gedit /usr/lib/nagios/plugins/ check_web_online
$ sudo chmod a+x /usr/lib/nagios/plugins/check_web_online
```

```

1#!/usr/bin/perl
2use strict;
3use warnings;
4
5my $online = int(`netstat -tn 2>/dev/null | grep :80 | awk '{print \$5}' | cut -d: -f1 | sort | uniq -c | sort -nr | head | wc -l`);
6
7if($online >= 0 and $online <= 400){
8    print "OK - online: $online\n";
9    exit 0;
10}
11elsif($online > 400 and $online <= 500){
12    print "WARNING - online: $online\n";
13    exit 1;
14}
15elsif($online > 500){
16    print "CRITICAL - online: $online\n";
17    exit 2;
18}
19else{
20    print "UNKNOWN\n";
21    exit 3;
22}

```

- Cấu hình trên Ubuntu Server

```

$ sudo gedit /etc/nagios/nrpe_local.cfg
Thêm dòng sau:
command[check_web_online]=usr/lib/nagios/plugins/ check_web_online
google.com

```

- Khởi động lại nrpe

```

$ sudo systemctl restart nagios-nrpe-server

```

- Trên Nagios Server thêm service

```

$ sudo gedit /etc/nagios4/servers/nagiosclient.cfg
Thêm dòng sau:
define service {
    host_name                trg-vm
    service_description      Check web online
    check_command             check_nrpe!check_web_online -t 30
    max_check_attempts       2
    check_interval            0.1
    retry_interval            0.1
    check_period              24x7
    check_freshness           1
    contact_groups            admins
    notification_interval     2
    notification_period       24x7
    notifications_enabled     1
    register                  1
}

```

- Khởi động lại nagios server

```
$ sudo systemctl restart nagios4.service
```

- Kiểm tra lại các plugin đã tạo trên giao diện web

Check domain expiration date	OK	12-21-2022 22:48:19	27d 22h 50m 48s	1/2	OK - "google.com" 2093 days left to expire.
Check net pyshark	CRITICAL	12-21-2022 22:48:07	0d 0h 0m 41s	1/10	CRITICAL - Possible DDoS Attack Type SYN flood!
Check web online	OK	12-21-2022 22:48:47	28d 0h 39m 3s	1/2	OK - online: 10