**Answer**

**2. (A)**

firewall-cmd --permanent --add-icmp-block-inversion

firewall-cmd --permanent --add-icmp-block=echo-reply

firewall-cmd --permanent --add-icmp-block=echo-request

firewall-cmd --reload

**2. (B)**

firewall-cmd –zone=private --add-rich-rule='rule family=ipv4 source address=192.168.1.0/24 service name=ssh log prefix="SSH Access" level="notice" accept'

**2. (C)**

firewall-cmd --zone=public --add-service=https

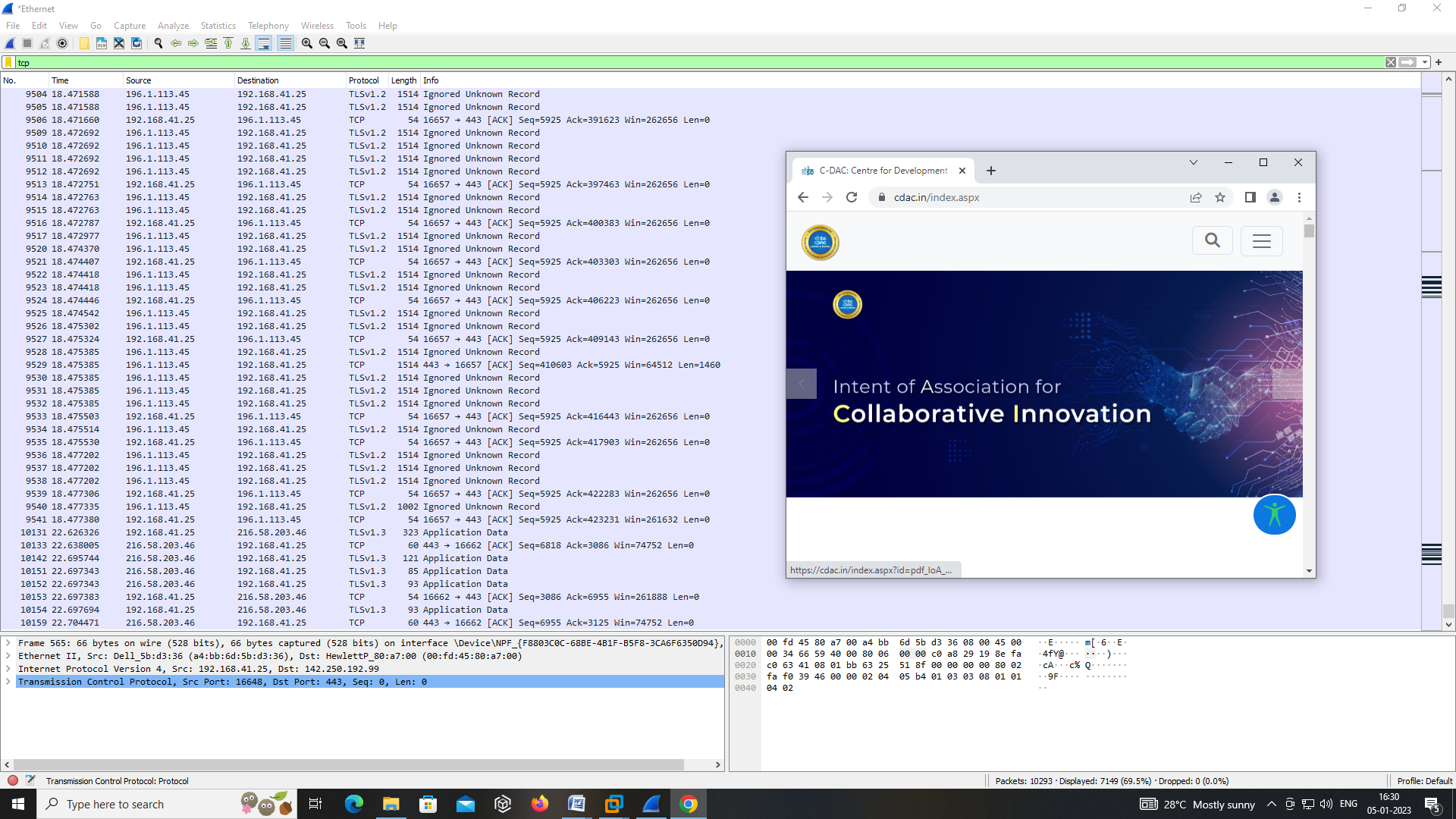
firewall-cmd --zone=public --permanent --add-service=https

firewall-cmd --reload

**3.**

**Steps:-**

Open Wireshark :- Select Ethernet and Click on Start Capture :- Open Web Browser and open any web url eg:- www.cdac.in Base Machine. Then open wireshark and search **tcp** Now we will be able to see Web Traffic.



**4. Ans**

**Set up Steps:-**

Create 4 VM Name as:- SERVER-1 NGINX , SERVER-2 NGINX, SERVER-3 NGINX

and put 3 VM on host only and add two interface NAT and, Host Only to 4th machine (NGINX).

SERVER-1 NGINX:- Put on Host Only and configure manual ip 10.1.1.2

SERVER-1 NGINX:- Put on Host Only configure manual ip 10.1.1.3

SERVER-1 NGINX:- Put on Host Only configure manual ip 10.1.1.4

NGINX:- Add two Nadwork Adaptor (NAT and Host Only)

**In SERVER-1 NGINX:-**

yum install httpd

systemctl start httpd

systemctl status httpd

systemctl status firewalld

firewall-cmd --list-all

firewall-cmd --add-port=80/tcp --permanent

cd /var/www/html

vim index.html

“**This is First NGINX- SERVER**”

**In SERVER-2 NGINX:-**

yum install httpd

systemctl start httpd

systemctl status httpd

systemctl status firewalld

firewall-cmd --list-all

firewall-cmd --add-port=80/tcp --permanent

cd /var/www/html

vim index.html

“**This is Second NGINX- SERVER**”

**In SERVER-3 NGINX:-**

yum install httpd

systemctl start httpd

systemctl status httpd

systemctl status firewalld

firewall-cmd --list-all

firewall-cmd --add-port=80/tcp --permanent

cd /var/www/html

vim index.html

“**This is Third NGINX- SERVER**”

**In NGINX:-**

yum install nginx

systemctl confstart nginx.service

cd /etc/nginx/nginx.conf

vim nginx.conf

--------------------------------------

add these lines at Line No. 37

-------------------------------------

upstream cluster1 {

server 10.1.1.2;

server 10.1.1.3;

server 10.1.1.4;

}

-------------------------------------

add these lines at Line No. 59:

-------------------------------------

location = /vlsi {

proxy\_pass http://cluster1/;

}

location = /dac {

proxy\_pass http://10.1.1.2/;

}

location = /hpcsa {

proxy\_pass http://10.1.1.3/;

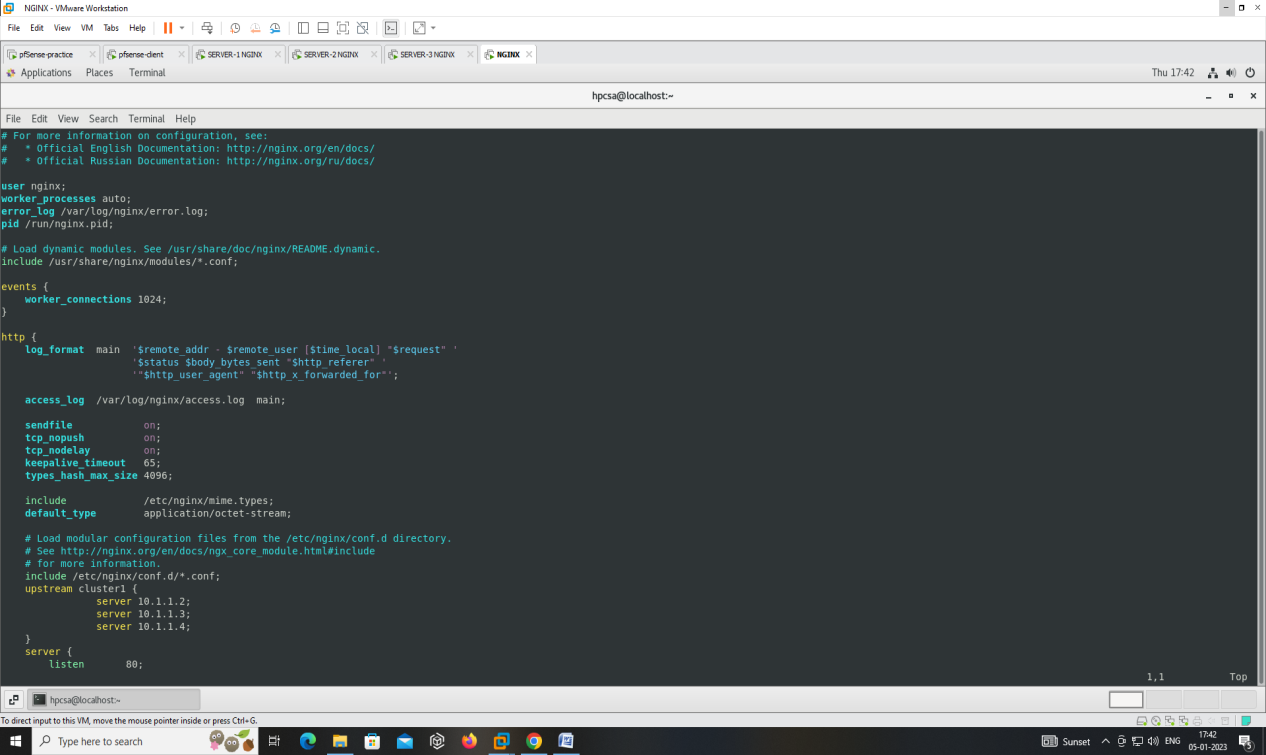
}

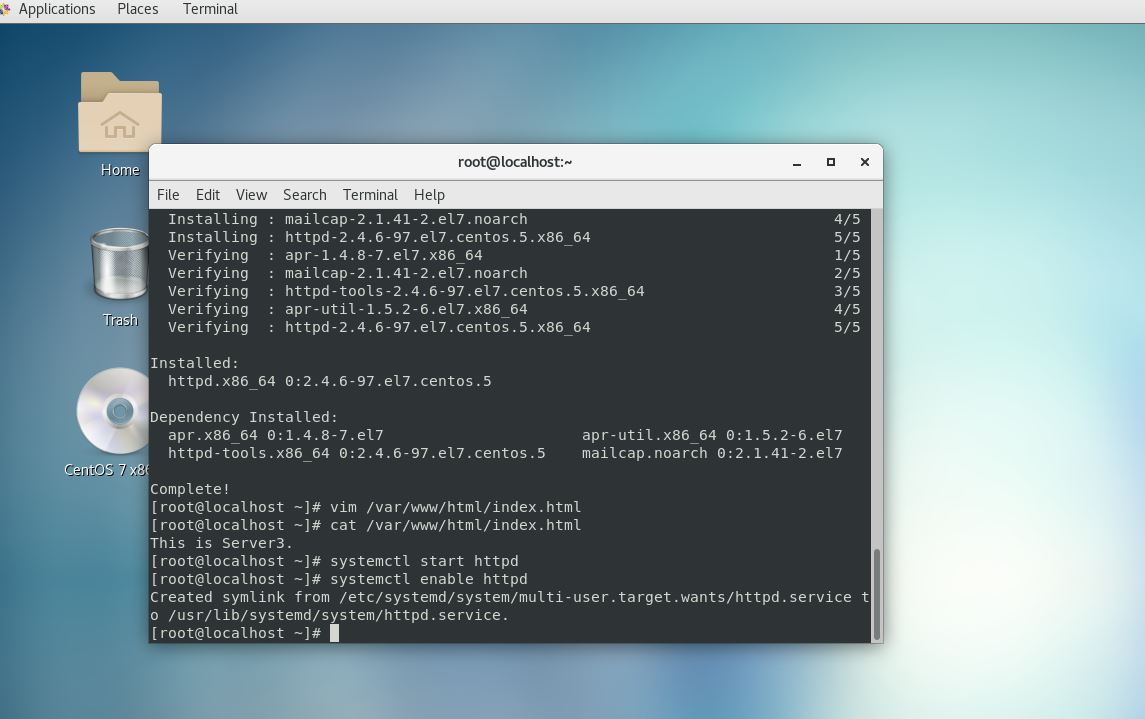
location = /iot {

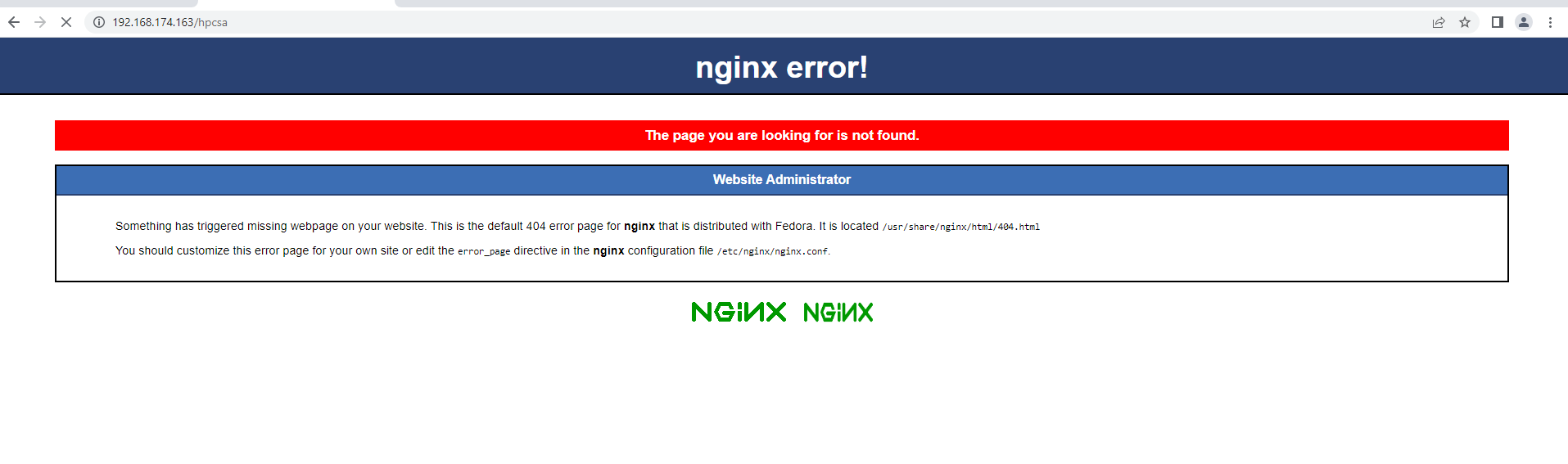
proxy\_pass http://10.1.1.4/;

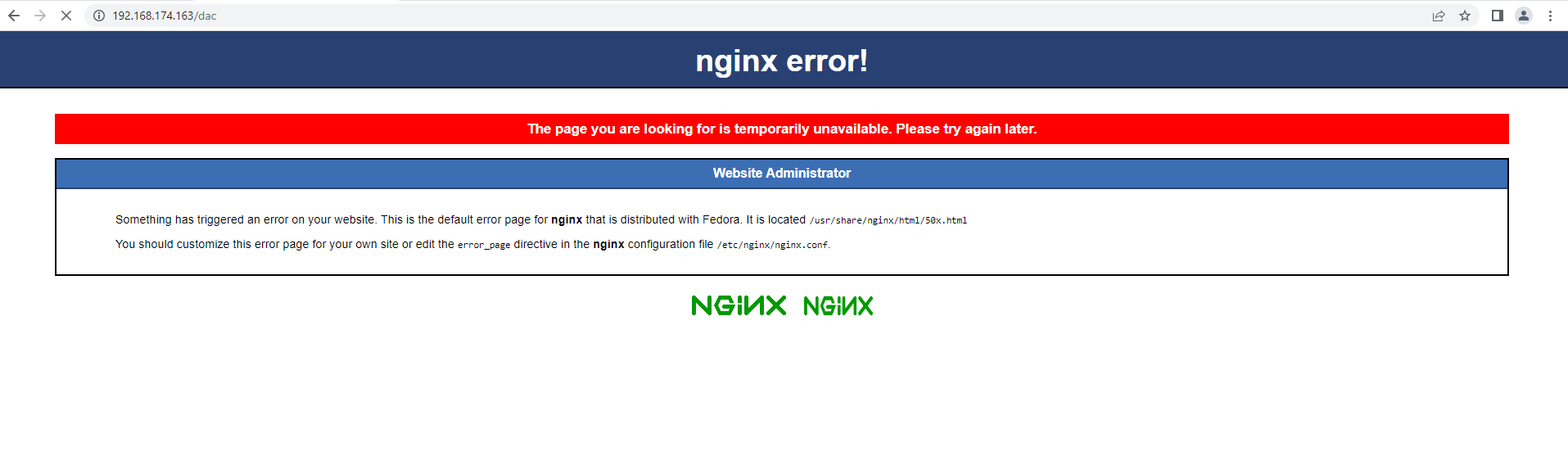
}

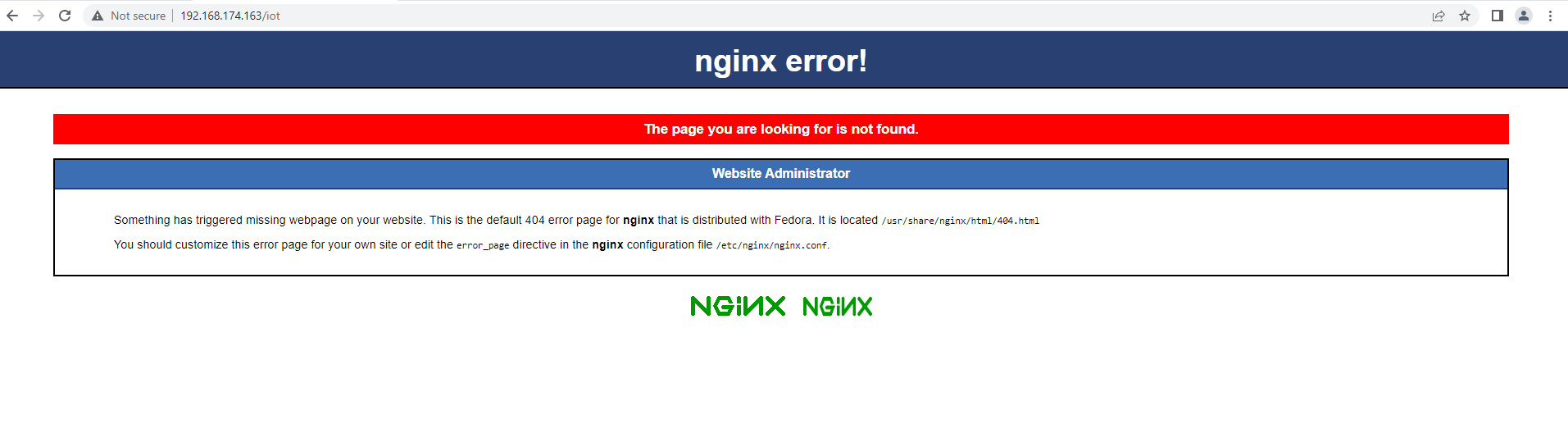
**systemctl restart nginx.service**











**6. Ans**

* **Snort Detect Incoming rule for SSH :-**

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 80 (msg:"SSH Accessed"; sid:1000007)

alert tcp any any -> any 22 (msg:"SSH Accessed"; sid:1000008)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 22 (msg:"SSH Accessed"; sid:1000009)

* **Snort Configure Steps :-**

