**Checkpoint 2 documentation**

**VAN LINH HA**

**116592171**

Brief Contents

[I. Windows Server Software Installation and Configuration 1](#_Toc535417548)

[a. ISS (Web Server) 1](#_Toc535417549)

[b. HMAIL 2](#_Toc535417550)

[c. DHCP 2](#_Toc535417551)

[d. DNS 2](#_Toc535417552)

[e. FTP FileZilla 3](#_Toc535417553)

[f. MYSQL Server 3](#_Toc535417554)

[II. Client machine software installation and configuration 4](#_Toc535417555)

[a. MYSQL Client 4](#_Toc535417556)

[b. Mail Client 4](#_Toc535417557)

[c. Install software: 4](#_Toc535417558)

[d. Grant permission to non-root user 4](#_Toc535417559)

[e. Traceroute 4](#_Toc535417560)

[III. Linux Server Software Installation And Configuration 6](#_Toc535417561)

[a. Apache 6](#_Toc535417562)

[b. SSH Service 7](#_Toc535417563)

[IV. Router Software Installation and Configuration 8](#_Toc535417564)

[a. DHCP Relay 8](#_Toc535417565)

[b. Routing 8](#_Toc535417566)

[c. IPTABLES 9](#_Toc535417567)

[d. SSH Service 11](#_Toc535417568)

[e. Nmap Service 11](#_Toc535417569)

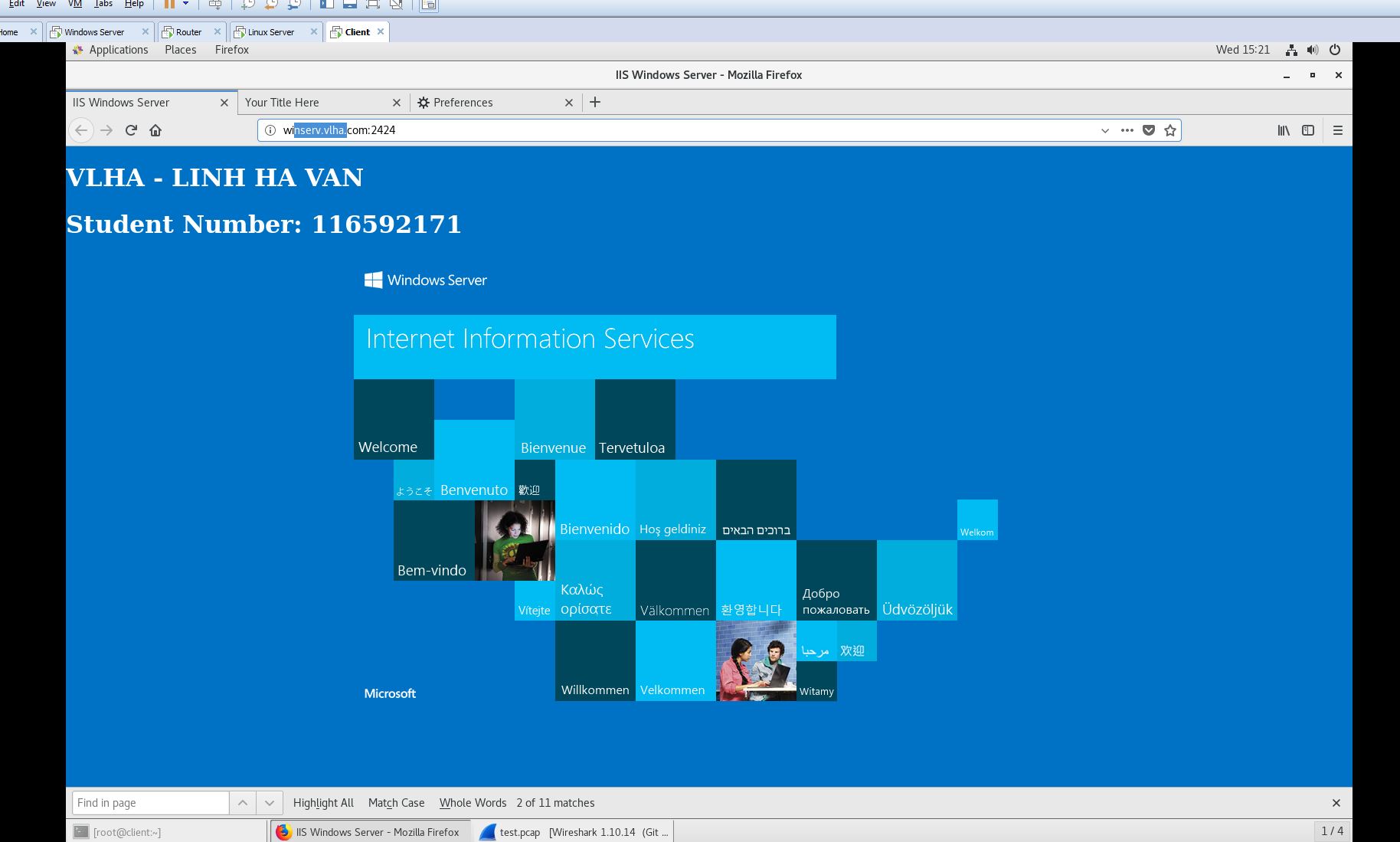
[f. Tcpdump Test 12](#_Toc535417570)

# 

# Windows Server Software Installation and Configuration

## ISS (Web Server)

* Login to Windows Server and open Server Manager
* Click Add Roles and Features on the Dashboard
* Click Next until reaching page Server Roles
* Choose Web Server (IIS), click Accept
* Click Next and then Install
* In Server Manager Dashboard, choose Tools -> Internet Information Services (ISS) Manager.
* Expand the pane until getting Default Web Site
* In the right pane click Bindings
* Choose the first line and click Edit on the popup on the screen
* Change the Host Name to winserv.vlha.com and Port to 2424
* Close the popup and click restart to restart the service.



## HMAIL

* Installation:
* Download hMail Server from website
* Run the file, agree to the terms
* Set admin password when installing

## DHCP

* Login to Windows Server and open Server Manager
* Click Add Roles and Features on the Dashboard
* Click Next until reaching page Server Roles
* Choose DHCP Server click Accept
* Click Next and then Install
* Open DHCP in Tools Server Manager
* Expand and right click on IPv4 and choose New Scope
* Type NDD in the Scope Name and click Next
* In the IP Address Range, put these following information into the box:
  + Start IP Address: 195.165.17.1
  + End IP Address: 195.165.17.62
  + Length: 24
* Click Next and Finish

## DNS

* Login to Windows Server and open Server Manager
* Click Add Roles and Features on the Dashboard
* Click Next until reaching page Server Roles
* Choose DNS Server click Accept
* Click Next and then Install
* Open DNS in Tools Server Manager
* Expand the left pane under DNS
* Right click Forward Lookup Zones and choose New Zone to create a new Forward Lookup Zone
* Keep everything default and click Next until getting Zone Name
* In the box, type vlha.com as a new zone and click Finish
* Add Hosts
* Right click onto Zone which was just created
* Choose New host (A or AAAA)
* Enter the name and IP address of the hosts need to be added, click onto the checkbox to add reserve IP addresses

## FTP FileZilla

* Download FileZilla Server from FileZilla Website
* Double Click to install
* Leave everything as default

## MYSQL Server

* Download MYSQL Server from the Internet
* Double click to install MYSQL
* Choose MYSQL Server when starting installing
* Click Next and Finish

# Client machine software installation and configuration

## MYSQL Client

* Download MYSQL from Website
* Double click to the installation file
* Set everything as default
* Choose MYSQL Workbench to install as MYSQL Client

## Mail Client

* Download and Install Thunderbird by this command :

**Yum install thunderbird**

## Install software:

* Open terminal and type these commands

**Yum install epel-release**

**Yum install –y tcpdump wireshark nmap**

**Yum update –y && yum upgrade –y**

## Grant permission to non-root user

* Open terminal and type these commands

**Chmod +s /usr/sbin/tcpdump**

**Chmod +s /usr/sbin/dumpcap**

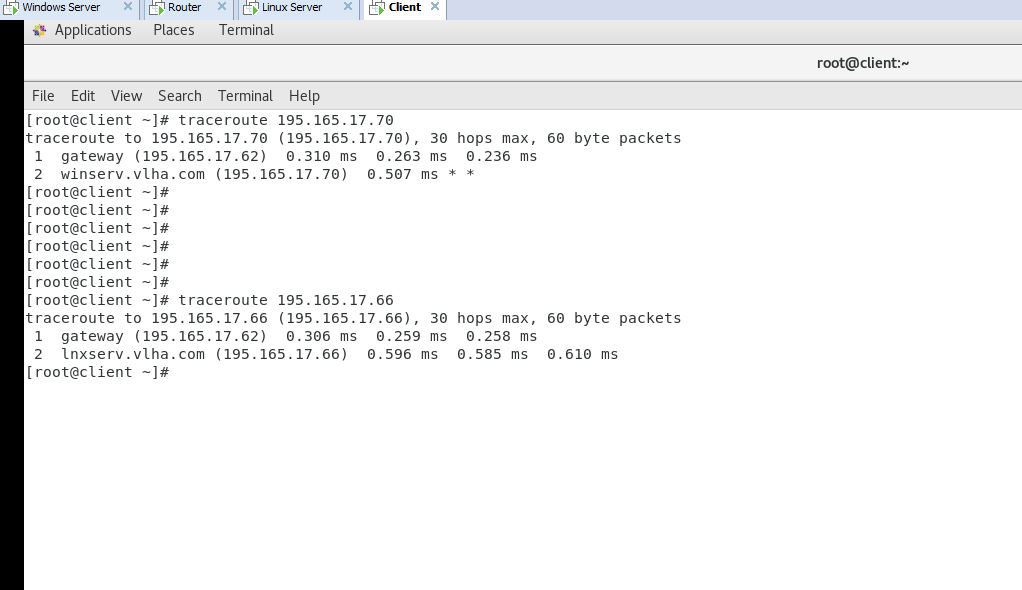
**Chmod +s /usr/sbin/thunderbird**

## Traceroute

* Open terminal and type these commands traceroute to LnxSer and Winserver:

**Traceroute 195.165.17.70**

**Traceroute 195.165.17.66**



# Linux Server Software Installation and Configuration

## Apache

* Download and install apache package by this command:

**Yum install -y httpd**

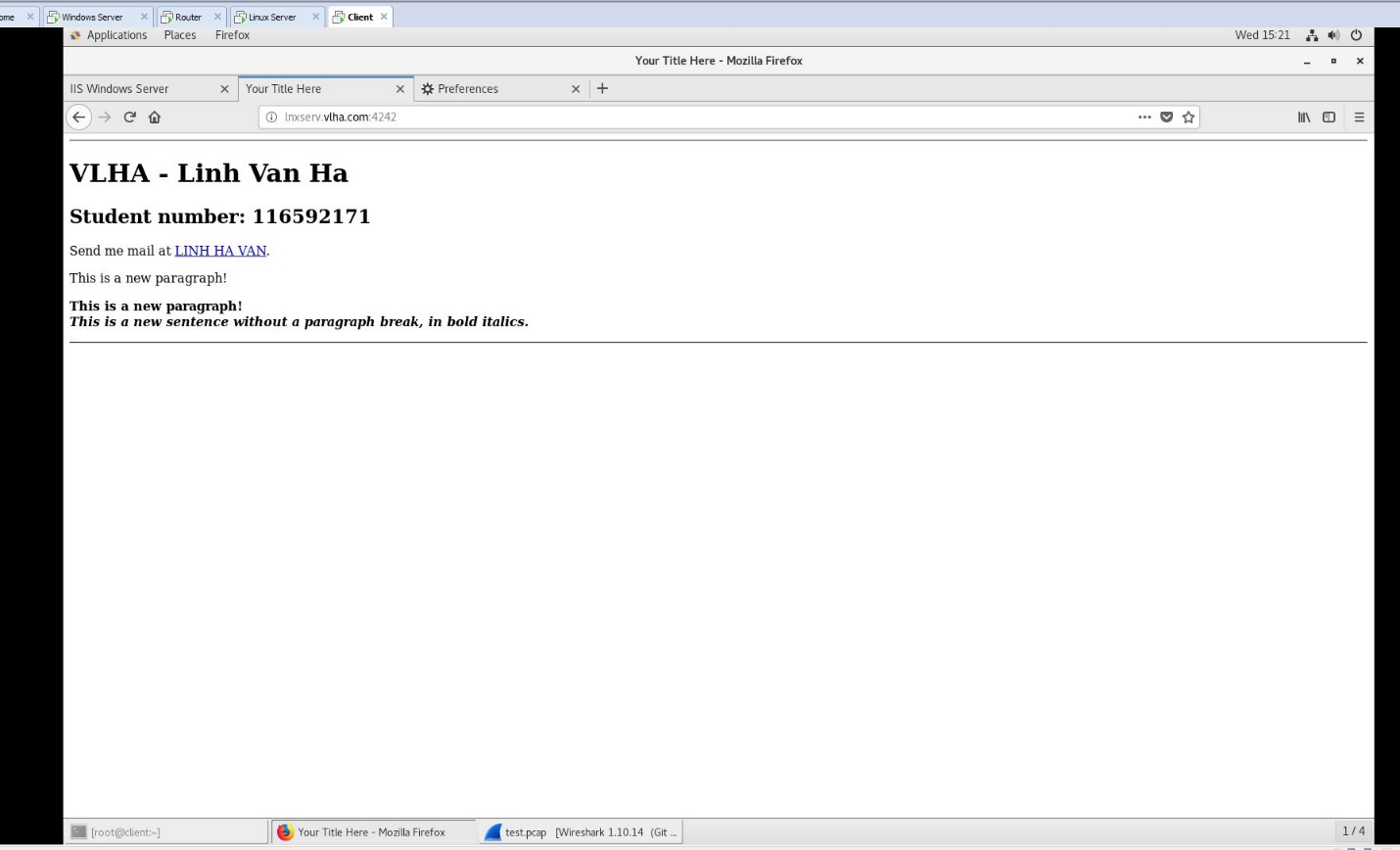
* Enable and start apache service

**Systemctl enable httpd**

**Systemctl start httpd**

* **Configuration**
* Edit the config file: /etc/httpd/conf/httpd.conf
* Uncomment line which has Listen 80 to Listen 4242
* Save the file and restart the service by this command:

**Systemctl restart httpd**

****

## SSH Service

* By default, Centos 7 already have installed SSH Server
* Edit the file: /etc/ssh/sshd\_config
* Locate the file which has # Port 22
* Uncomment the line and change to Port 7373
* Restart the service by this command

**Systemctl restart sshd**

# Router Software Installation and Configuration

## DHCP Relay

* Download and install DHCP package by running this command:

**Yum install dhcp**

* Configuration
* Copy file dhcprelay.service to the path: /etc/systemd/system/
* Edit the file in the new location: /etc/system/system/dhcprelay.service
* Locate the “ExecStart” and change to:

**ExecStart=/usr/sbin/dhcrelay -d --no-pid DHCP\_SERVER\_IPADDR -i Interface\_receive\_DHCP\_request**

* Restart dhcp relay service

**systemctl --system daemon-reload**

**systemctl restart dhcrelay**

****

## Routing

* Edit the file :/etc/sysctl.conf
* Append this command to the end of the file

**net.ipv4.ip\_forward=1**

* Save the file and restart network

## IPTABLES

#!/bin/bash

iptables -t filter -F

iptables -X

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP

**# Apache service**

iptables -N APACHE

iptables -A FORWARD -p tcp -s 195.165.17.0/26 --dport 4242 -m state --state NEW,ESTABLISHED,RELATED -j APACHE

iptables -A FORWARD -p tcp -d 195.165.17.0/26 --sport 4242 -m state --state ESTABLISHED,RELATED -j APACHE

iptables -A APACHE -j LOG --log-prefix "APACHE"

iptables -A APACHE -j ACCEPT

**# ISS service**

iptables -N ISS

iptables -A FORWARD -p tcp -s 195.165.17.0/26 --dport 2424 -m state --state NEW,ESTABLISHED,RELATED -j ISS

iptables -A FORWARD -p tcp -d 195.165.17.0/26 --sport 2424 -m state --state ESTABLISHED,RELATED -j ISS

iptables -A ISS -j LOG --log-prefix "ISS"

iptables -A ISS -j ACCEPT

**# DNS service**

iptables -N DNS

iptables -A FORWARD -p tcp -s 195.165.17.0/26 --dport 53 -m state --state NEW,ESTABLISHED,RELATED -j DNS

iptables -A FORWARD -p tcp -s 195.165.17.0/24 --sport 53 -m state --state NEW,ESTABLISHED,RELATED -j DNS

iptables -A FORWARD -p udp -s 195.165.17.0/26 --dport 53 -m state --state NEW,ESTABLISHED,RELATED -j DNS

iptables -A FORWARD -p udp -s 195.165.17.0/24 --sport 53 -m state --state NEW,ESTABLISHED,RELATED -j DNS

iptables -A DNS -j LOG --log-prefix "DNS"

iptables -A DNS -j ACCEPT

**# DHCP service**

iptables -N DHCP

iptables -A INPUT -p udp --dport 67:68 -m state --state NEW,ESTABLISHED,RELATED -j DHCP

iptables -A OUTPUT -p udp --sport 67:68 -m state --state NEW,ESTABLISHED,RELATED -j DHCP

iptables -A FORWARD -p udp --dport 67:68 -m state --state NEW,ESTABLISHED,RELATED -j DHCP

iptables -A FORWARD -p udp --sport 67:68 -m state --state NEW,ESTABLISHED,RELATED -j DHCP

iptables -A DHCP -j LOG --log-prefix "DHCP"

iptables -A DHCP -j ACCEPT

**# Traceroute**

iptables -N TRACEROUTE

iptables -A OUTPUT -p icmp -j TRACEROUTE

iptables -A FORWARD -p icmp -j TRACEROUTE

iptables -A OUTPUT -p udp --dport 33434:33474 -j TRACEROUTE

iptables -A FORWARD -p udp --dport 33434:33474 -j TRACEROUTE

iptables -A TRACEROUTE -j LOG --log-prefix "TRACEROUTE" --log-level 4

iptables -A TRACEROUTE -j ACCEPT

## SSH Service

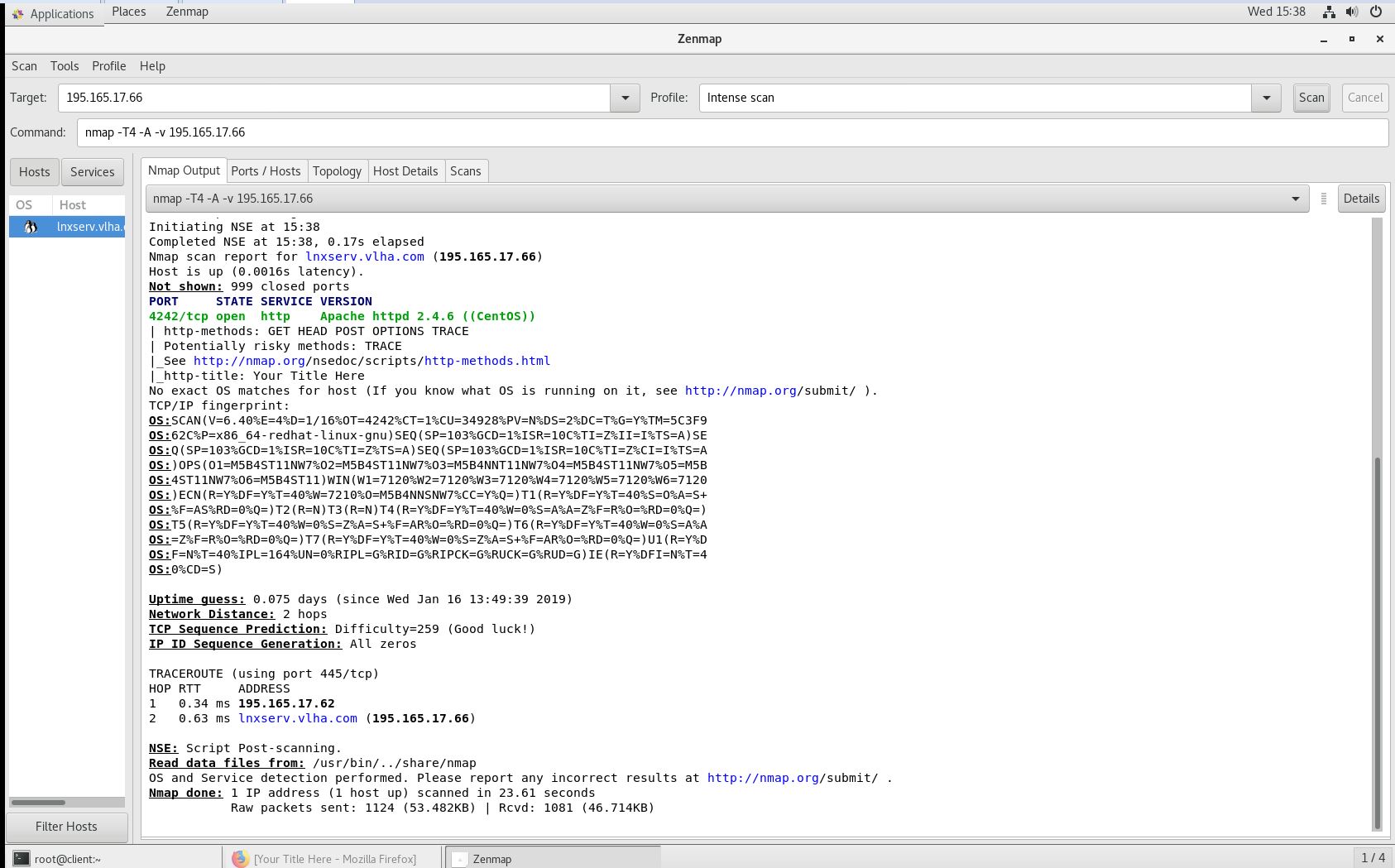
* By default, Centos 7 already have installed SSH Server
* Edit the file: /etc/ssh/sshd\_config
* Locate the file which has # Port 22
* Uncomment the line and change to Port 7373
* Restart the service by this command

**Systemctl restart sshd**

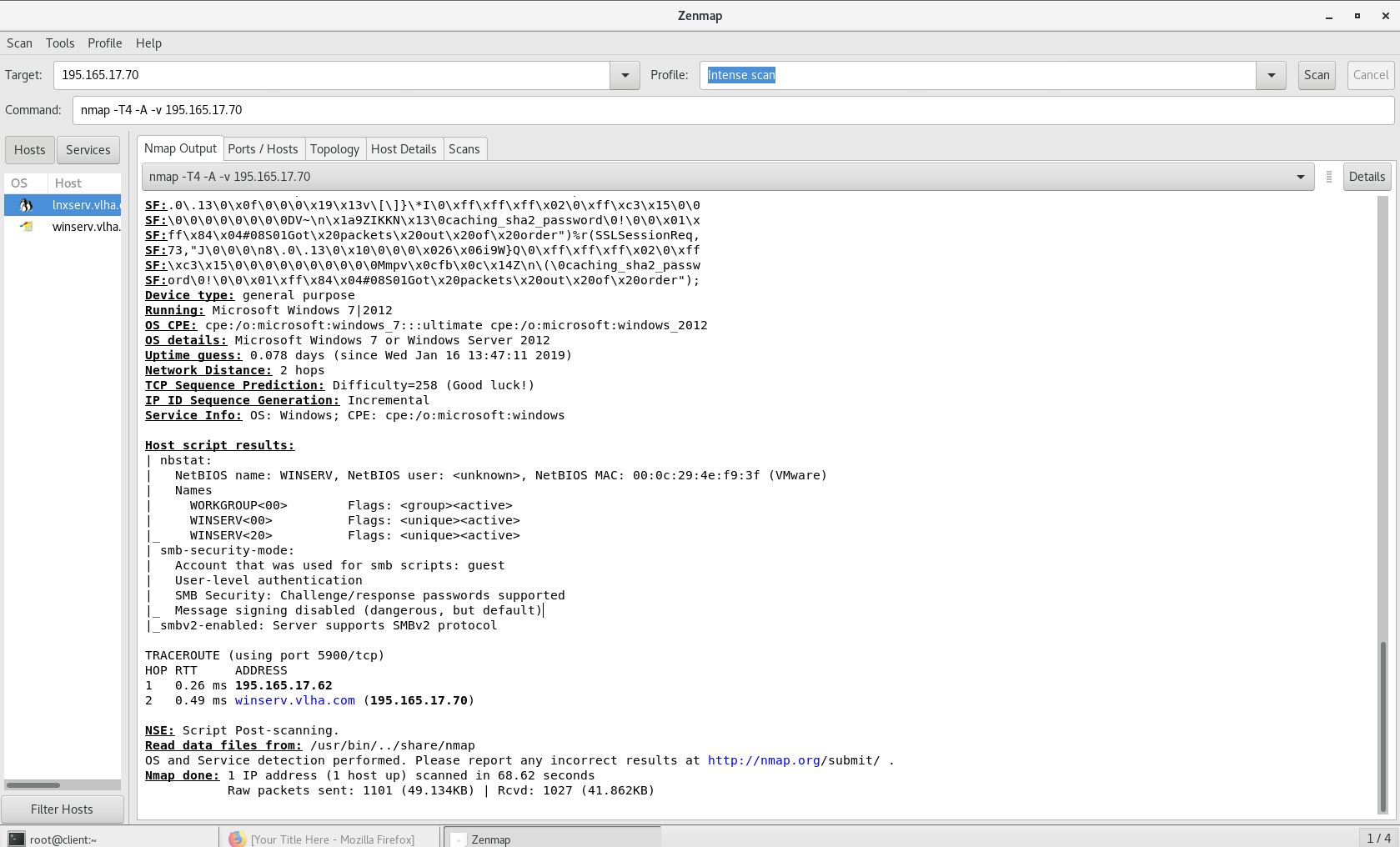
## Nmap Service

* To run network scan, open terminal and run this command

**nmap -T4 -A -v 195.165.17.66 (scan Linux Server)**

****

**nmap -T4 -A -v 195.165.17.70 (scan Windows Server)**

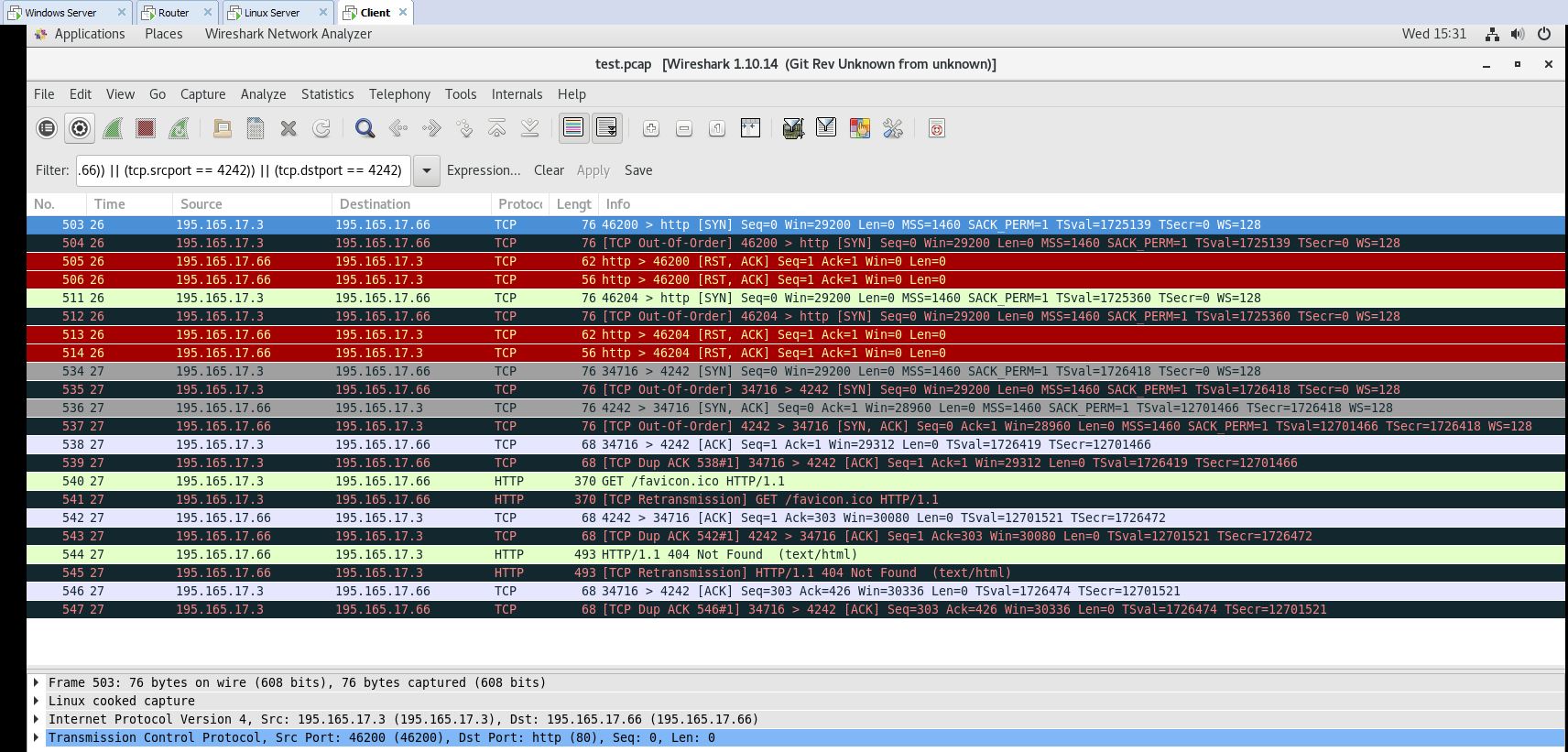
****

## Tcpdump Test

* To be able to run tcpdump to listen the traffic on all the interfaces and save it to the file which has extension pcap. Open the terminal then run this command

**Tcpdump –i any –w file\_name.pcap**

* Copy the file you just created and move to the client. Open Wireshark and type this command into the filter

**(((ip.src == 195.165.17.66) || (ip.dst == 195.165.17.66)) || (tcp.srcport == 4242)) || (tcp.dstport == 4242)**