**Checkpoint 3 documentation**

**VAN LINH HA**

**116592171**

Brief Contents

[I. Windows Server Services Configuration 1](#_Toc535872121)

[a. Email Server 1](#_Toc535872122)

[b. FTP Server 1](#_Toc535872123)

[c. MYSQL Server 1](#_Toc535872124)

[II. Client Machine Services Configuration 3](#_Toc535872125)

[a. MYSQL Client 3](#_Toc535872126)

[b. Mail Client 3](#_Toc535872127)

[c. FTP Client 3](#_Toc535872128)

[d. SSH/SCP Client 3](#_Toc535872129)

[e. Nmap Client 4](#_Toc535872130)

[III. Linux Server Services Configuration 5](#_Toc535872131)

[a. SSH/SCP Service 5](#_Toc535872132)

[IV. Router Services Configuration 6](#_Toc535872133)

[a. SSH Service 6](#_Toc535872134)

[b. IPTABLES 6](#_Toc535872135)

[**c.** **IPLOG SCRIPT** 14](#_Toc535872136)

[d. Nmap Service 14](#_Toc535872137)

[e. Tcpdump Test 15](#_Toc535872138)

# Windows Server Services Configuration

## Email Server

* After installing HMail server, a hmail icon will be appear on the Desktop.
* Start hMail Server administrator.
* Type administrator password in the popup on the windows
* Click Ok
* Click Add Domain in the left pane
* Enter yoursenecaid.com (domain name) and click save
* Choose Add account, click add new email account
* Type your senecaid and password, click Save
* In Setting, choose protocol SMTP then choose the Delivery of email tab
* In the Hostname, use your domain name

## FTP Server

* Double click FileZilla Server on the Desktop
* In the top pane, choose Edit, then Users
* On the right side, click Add
* Type your regular user and password in the popup screen
* Go back to the main screen, redo click on Edit, choose Settings
* On the left pane, click on Passive Mode Settings
* Choose the box Custom Port Range and enter 20 into the box
* Click Ok to finish

## MYSQL Server

* Open Windows Start, type MYSQL Workbench, click to open the application
* Choose Local Instance MYSQL Router to login to the MYSQL Database
* In the bottom left pane, right click to create schema
* Type the name of the schema and click Apply
* A confirmation box will show up on the screen
* Click Apply and then Finish
* When it’s done, the newly schema will be showed in the left pane under Schema section
* Double click on the newly schema
* In the top bar, choose Server then Users and Privileges
* Type username and password in the right pane and click Apply
* Go to Scheme Privileges to give user permission
* Choose Add Entry and choose your database
* Select permissions for user
* Click Apply

# Client Machine Services Configuration

## MYSQL Client

* Open MYSQL Workbench in Application -> Programming
* Click Connect to Server
* Type administrator password
* In the main console, use select command

**Show tables from database\_name;**

## Mail Client

* Open thunderbird in Application -> Internet
* Open Mail Account Setup
* Put Full Name, user1@yoursenecaid.com, password
* Click Manual Configuration
* Type winserv.yoursenecaid.com in Incoming box for IMAP setup with the port is 143 and None SSL
* Type winserv.yoursenecaid.com in Outgoing box for SMTP setup with the port is 25 and None SSL
* Click Done => Understand the risk and click Ok

Repeat all the above steps for user2

## FTP Client

* Open Application => Internet => FileZilla
* Enter the hostname which is the FTP Server
* Enter Username and password which were created before
* Put port 21 and click connect to the server
* On the right pane is the list directory of FTP server
* Right click to the random file and choose Download

## SSH/SCP Client

* Open terminal and type these commands

**Ssh -p 7373 lnxserv.yoursenecaid.com**

**Scp -P 7373 lnxserv.yoursenecaid.com:/root/testfile.txt .**

## Nmap Client

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

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

# Linux Server Services Configuration

## SSH/SCP 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 Services Configuration

## 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 3737
* Restart the service by this command

**Systemctl restart sshd**

## IPTABLES

**\*\*\* Scenerio 1a**

#!/bin/bash

iptables -t filter -F

iptables -X

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP

iptables -N INPUT-ACCEPT

iptables -N INPUT-DROP

iptables -N OUTPUT-ACCEPT

iptables -N OUTPUT-DROP

iptables -N FORWARD-ACCEPT

iptables -N FORWARD-DROP

iptables -A INPUT -j INPUT-DROP

iptables -A OUTPUT -j INPUT-DROP

iptables -A FORWARD -j INPUT-DROP

#Rules for INPUT-ACCEPT chain

iptables -A INPUT-ACCEPT -j LOG --log-prefix "INPUT-ACCEPTED"

iptables -A INPUT-ACCEPT -j ACCEPT

#Rules for INPUT-DROP chain

iptables -A INPUT-DROP -j LOG --log-prefix "INPUT-DROPPED"

iptables -A INPUT-DROP -j DROP

#Rules for OUPUT-ACCEPT chain

iptables -A OUTPUT-ACCEPT -j LOG --log-prefix "OUTPUT-ACCEPTED"

iptables -A OUTPUT-ACCEPT -j ACCEPT

#Rules for OUTPUT-DROP chain

iptables -A OUTPUT-DROP -j LOG --log-prefix "OUTPUT-DROPPED"

iptables -A OUTPUT-DROP -j DROP

#Rules for FORWARD-ACCEPT chain

iptables -A FORWARD-ACCEPT -j LOG --log-prefix "FORWARD-ACCEPTED"

iptables -A FORWARD-ACCEPT -j ACCEPT

#Rules for FORWARD-DROP chain

iptables -A FORWARD-DROP -j LOG --log-prefix "FORWARD-DROPPED"

iptables -A FORWARD-DROP -j DROP

#SSH/SCP to Router

iptables -A INPUT -p tcp -s 195.165.17.0/26 --dport 3737 -m state --state NEW,ESTABLISHED,RELATED -j INPUT-ACCEPT

iptables -A OUTPUT -p tcp -d 195.165.17.0/26 --sport 3737 -m state --state ESTABLISHED,RELATED -j OUTPUT-ACCEPT

#SSH/SCP to Server

iptables -A FORWARD -p tcp -s 195.165.17.0/26 --dport 7373 -m state --state NEW,ESTABLISHED,RELATED -j FORWARD-ACCEPT

iptables -A FORWARD -p tcp -d 195.165.17.0/26 --sport 7373 -m state --state ESTABLISHED,RELATED -j FORWARD-ACCEPT

#IIS

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

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

#Apache

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

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

#MySQL

iptables -A FORWARD -p tcp -s 195.165.17.0/26 --dport 3306 -m state --state NEW,ESTABLISHED,RELATED -j FORWARD-ACCEPT

iptables -A FORWARD -p tcp -d 195.165.17.0/26 --sport 3306 -m state --state ESTABLISHED,RELATED -j FORWARD-ACCEPT

#HMAIL IMAP

iptables -A FORWARD -p tcp -s 195.165.17.0/26 --dport 143 -m state --state NEW,ESTABLISHED,RELATED -j FORWARD-ACCEPT

iptables -A FORWARD -p tcp -d 195.165.17.0/26 --sport 143 -m state --state ESTABLISHED,RELATED -j FORWARD-ACCEPT

#HMAIL SMTP

iptables -A FORWARD -p tcp -s 195.165.17.0/26 --dport 25 -m state --state NEW,ESTABLISHED,RELATED -j FORWARD-ACCEPT

iptables -A FORWARD -p tcp -d 195.165.17.0/26 --sport 25 -m state --state ESTABLISHED,RELATED -j FORWARD-ACCEPT

#DNS

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

iptables -A FORWARD -p tcp -d 195.165.17.0/26 --sport 53 -m state --state ESTABLISHED,RELATED -j FORWARD-ACCEPT

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

iptables -A FORWARD -p udp -d 195.165.17.0/26 --sport 53 -m state --state ESTABLISHED,RELATED -j FORWARD-ACCEPT

#DHCP

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

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

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

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

#FTP UNENCRYPTED

iptables -A FORWARD -p tcp -s 195.165.17.0/26 --dport 21 -m state --state NEW,ESTABLISHED,RELATED -j FORWARD-ACCEPT

iptables -A FORWARD -p tcp -d 195.165.17.0/26 --sport 21 -m state --state ESTABLISHED,RELATED -j FORWARD-ACCEPT

iptables -A FORWARD -p tcp -s 195.165.17.0/26 --dport 20 -m state --state NEW,ESTABLISHED,RELATED -j FORWARD-ACCEPT

iptables -A FORWARD -p tcp -d 195.165.17.0/26 --sport 20 -m state --state ESTABLISHED,RELATED -j FORWARD-ACCEPT

**\*\*\* Scenerio 1b**

#!/bin/bash

iptables -t filter -F

iptables -X

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP

iptables -N INPUT-ACCEPT

iptables -N INPUT-DROP

iptables -N OUTPUT-ACCEPT

iptables -N OUTPUT-DROP

iptables -N FORWARD-ACCEPT

iptables -N FORWARD-DROP

iptables -A INPUT -j OUTPUT-DROP

iptables -A OUTPUT -j OUTPUT-DROP

iptables -A FORWARD -j OUTPUT-DROP

#Rules for INPUT-ACCEPT chain

iptables -A INPUT-ACCEPT -j LOG --log-prefix "INPUT-ACCEPTED"

iptables -A INPUT-ACCEPT -j ACCEPT

#Rules for INPUT-DROP chain

iptables -A INPUT-DROP -j LOG --log-prefix "INPUT-DROPPED"

iptables -A INPUT-DROP -j DROP

#Rules for OUPUT-ACCEPT chain

iptables -A OUTPUT-ACCEPT -j LOG --log-prefix "OUTPUT-ACCEPTED"

iptables -A OUTPUT-ACCEPT -j ACCEPT

#Rules for OUTPUT-DROP chain

iptables -A OUTPUT-DROP -j LOG --log-prefix "OUTPUT-DROPPED"

iptables -A OUTPUT-DROP -j DROP

#Rules for FORWARD-ACCEPT chain

iptables -A FORWARD-ACCEPT -j LOG --log-prefix "FORWARD-ACCEPTED"

iptables -A FORWARD-ACCEPT -j ACCEPT

#Rules for FORWARD-DROP chain

iptables -A FORWARD-DROP -j LOG --log-prefix "FORWARD-DROPPED"

iptables -A FORWARD-DROP -j DROP

#SSH/SCP to Router

iptables -A INPUT -p tcp -s 195.165.17.0/26 --dport 3737 -m state --state NEW,ESTABLISHED,RELATED -j INPUT-ACCEPT

iptables -A OUTPUT -p tcp -d 195.165.17.0/26 --sport 3737 -m state --state ESTABLISHED,RELATED -j OUTPUT-ACCEPT

#SSH/SCP to Server

iptables -A FORWARD -p tcp -s 195.165.17.0/26 --dport 7373 -m state --state NEW,ESTABLISHED,RELATED -j FORWARD-ACCEPT

iptables -A FORWARD -p tcp -d 195.165.17.0/26 --sport 7373 -m state --state ESTABLISHED,RELATED -j FORWARD-ACCEPT

#IIS

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

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

#Apache

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

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

#MySQL

iptables -A FORWARD -p tcp -s 195.165.17.0/26 --dport 3306 -m state --state NEW,ESTABLISHED,RELATED -j FORWARD-ACCEPT

iptables -A FORWARD -p tcp -d 195.165.17.0/26 --sport 3306 -m state --state ESTABLISHED,RELATED -j FORWARD-ACCEPT

#HMAIL IMAP

iptables -A FORWARD -p tcp -s 195.165.17.0/26 --dport 143 -m state --state NEW,ESTABLISHED,RELATED -j FORWARD-ACCEPT

iptables -A FORWARD -p tcp -d 195.165.17.0/26 --sport 143 -m state --state ESTABLISHED,RELATED -j FORWARD-ACCEPT

#HMAIL SMTP

iptables -A FORWARD -p tcp -s 195.165.17.0/26 --dport 25 -m state --state NEW,ESTABLISHED,RELATED -j FORWARD-ACCEPT

iptables -A FORWARD -p tcp -d 195.165.17.0/26 --sport 25 -m state --state ESTABLISHED,RELATED -j FORWARD-ACCEPT

#DNS

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

iptables -A FORWARD -p tcp -d 195.165.17.0/26 --sport 53 -m state --state ESTABLISHED,RELATED -j FORWARD-ACCEPT

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

iptables -A FORWARD -p udp -d 195.165.17.0/26 --sport 53 -m state --state ESTABLISHED,RELATED -j FORWARD-ACCEPT

#DHCP

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

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

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

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

#FTP UNENCRYPTED

iptables -A FORWARD -p tcp -s 195.165.17.0/26 --dport 21 -m state --state NEW,ESTABLISHED,RELATED -j FORWARD-ACCEPT

iptables -A FORWARD -p tcp -d 195.165.17.0/26 --sport 21 -m state --state ESTABLISHED,RELATED -j FORWARD-ACCEPT

iptables -A FORWARD -p tcp -s 195.165.17.0/26 --dport 20 -m state --state NEW,ESTABLISHED,RELATED -j FORWARD-ACCEPT

iptables -A FORWARD -p tcp -d 195.165.17.0/26 --sport 20 -m state --state ESTABLISHED,RELATED -j FORWARD-ACCEPT

1. **IPLOG SCRIPT**

**#!/bin/bash**

**#### LOG FILE ####**

**read -p "Log start from: " start**

**read -p "Log end: " end**

**read -p "Port: " port**

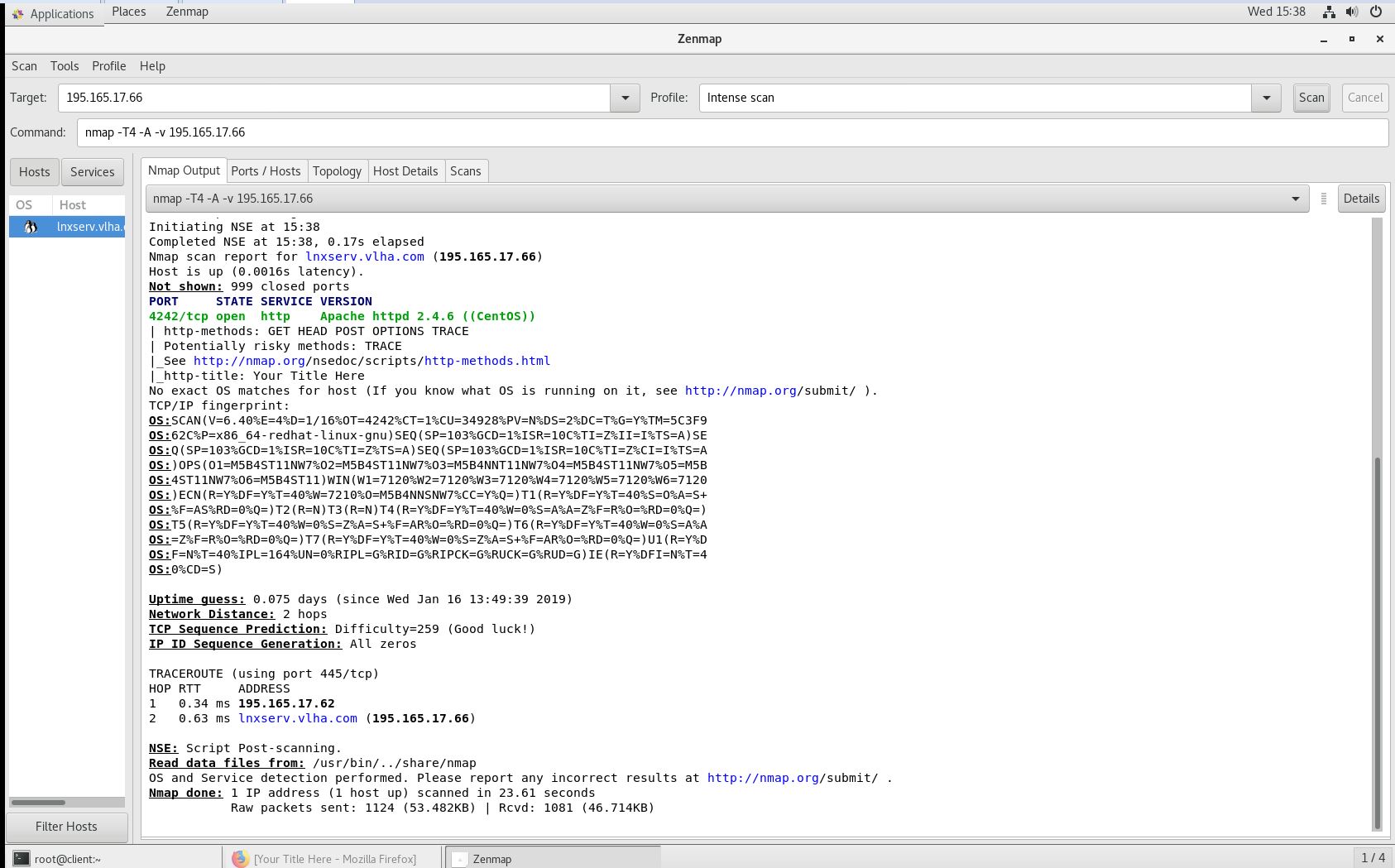
**read -p "Status: " status**

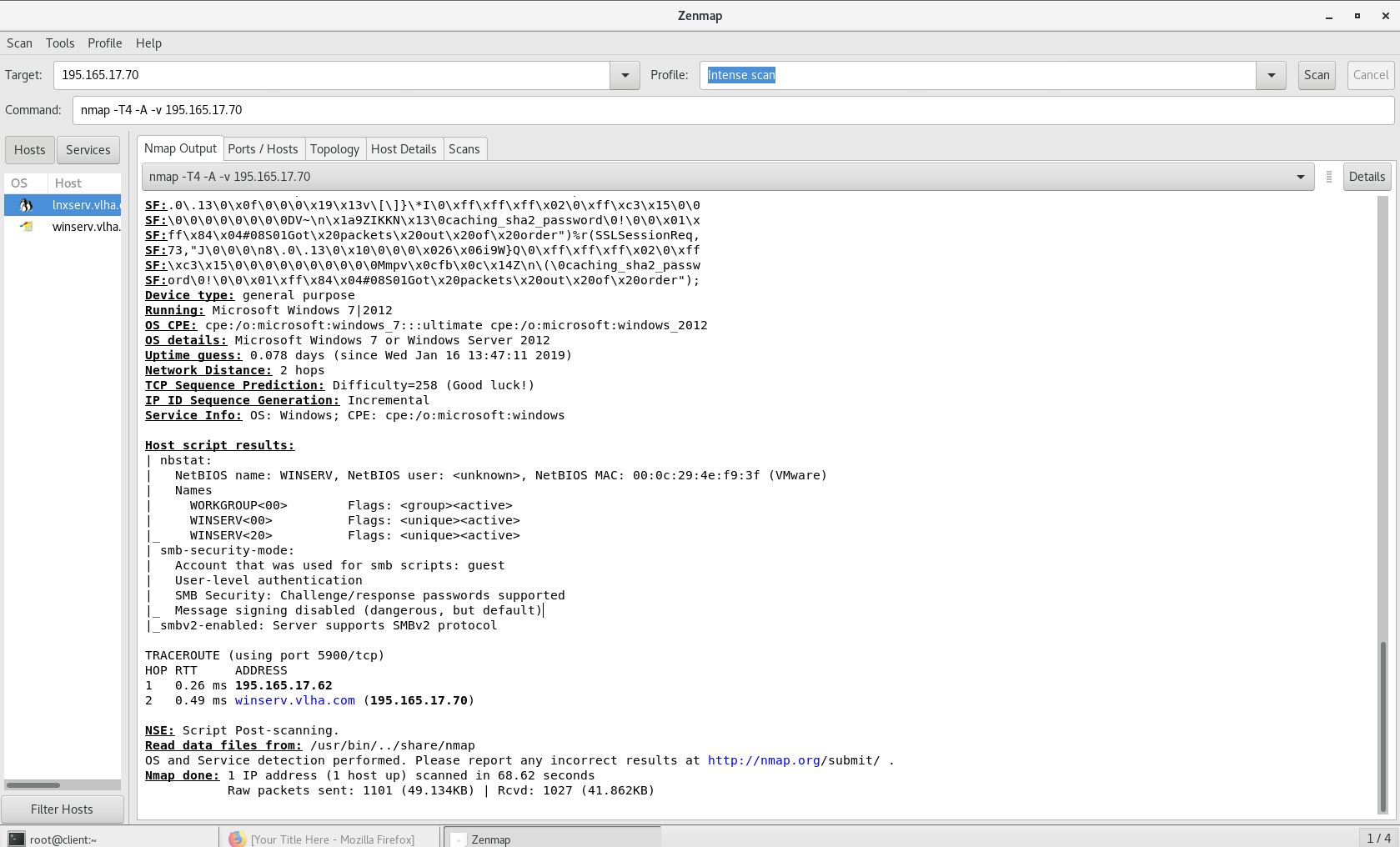
**awk -v t1="$start" -v t2="$end" 't1 <= $0 && $0 <=t2' /var/log/message | grep "$port" | grep "$status"**

## 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)**

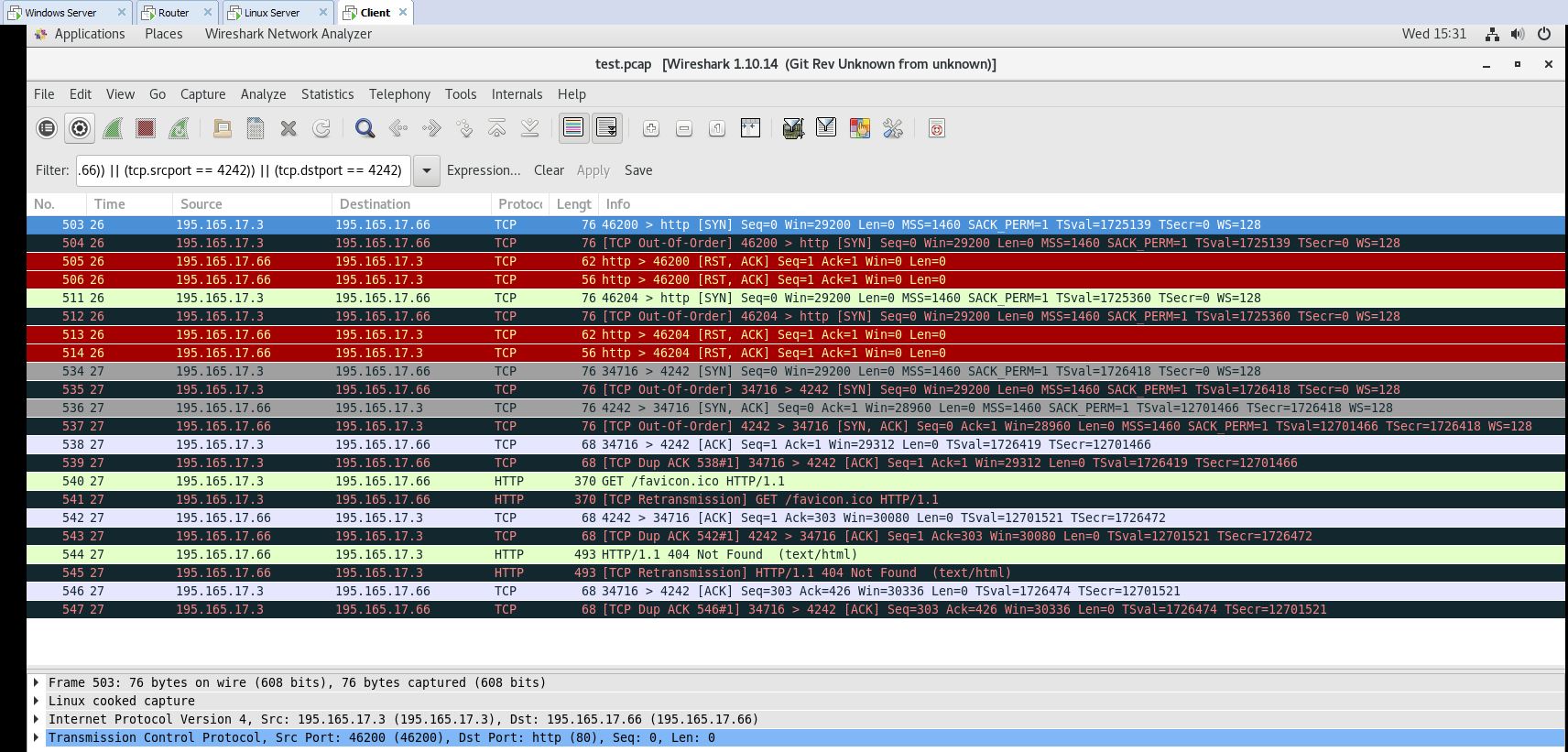
****

## 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)**