**Windows server configuration**

**1. DHCP configuration**

Change computer name to winserv

Installation

Server Manager -> Manage –> Add Roles -> Server Roles -> DHCP Server

DHCP manager -> Create DCHP Scope

Start ip address 172.16.20.65

End ip address 172.16.20.126

Exclusion 172.165.20.65 -172.165.20.100

Default gateway 172.165.20.126

**2. DNS**

**Installation**

Server Manager -> Manage –> Add Roles -> Server Roles -> DNS Server

Before configure DNS, change to static IP address same as DNS IP address

Configuring Domain name yhong39.com

**DNS Manager**

Create Forward Lookup Zone for staped.com

Create Host(A or AAAA) -> lnxserv, winserv with IP address

Create Reverse Lookup Zones

Put the IP address 172.16.20

Create CNAME for lnxserv, winserv

**3. IIS(Internet Information Service)**

**Installation**

Server Manager -> manage -> Add roles > server Roles -> Web Server(IIS)

Expand Server pane -> expand Sites -> right click Default Web Site -> Edit bindings -> add hostname to winserv.sapted.com and port number to 1515.

**4. FileZilla**

Download from the Internet FileZilla Server

Choose port number 21

**Linux Server Configuration and Installation**

**1.Apache**

Yum install -y httpd

Systemctl enable httpd

Systemctl start httpd

Install semanage -> policycoreutils-python-2.4-33.el7.x86\_64

Semanage port -a -t http\_port\_t -p tcp 5151

**Router Configuration and Installation**

**DHCP Relay**

**Yum install DHCP**

Cp /lib/systemd/system/dhcrelay.service /etc/systemd/system

Vi /etc/systemd/system/dhcrelay.service

Add your DHCP server IP address and the interface which is the client is connected with the router

ExecStart=/usr/sbin/dhcrelay -d --no-pid 172.16.20.5 -i ens38 -I ens37

**Restart dhcrelay service**

Systemctl –system daemon-reload

Systemctl restart dhcrealy

**Routing**

Vi /etc/sysctl.conf

Add net.ipv4.ip\_forward=1 in an empty space.

Run the command : sysctl -p /etc.sysctl.conf

Service network restart.

**Go to Client** tpye: dhclient -r ens36 -> dhclient ens36

**SSH(change port number)**

Semanage port –a –t ssh\_port\_t –p tcp 3535

**Client Configuration**

**Giving permission for user**

Chmod +s /usr/sbin/tcpdump

Chmod +s /usr/sbin/dumpcap

Chmod +s /usr/bin/filezilla

Chmod +s /usr/sbin/wireshark

**Renew DHCP IP address**

Dhclient -r

**Iptables**

#!/bin/bash

#Flush tables and set policies to drop

iptables -F

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP

iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE

#Create Logging Chain for accepted packets on INPUT CHAIN

iptables -N accept-input

#Rules for accept-input Chain

iptables -A accept-input -j LOG --log-prefix "INPUT-ACCEPTED"

iptables -A accept-input -j ACCEPT

#Create Logging Chain for dropped packets on INPUT CHAIN

iptables -N drop-input

#Rules for drop-input chain

iptables -A drop-input -j LOG --log-prefix "INPUT-DROPPED"

iptables -A drop-input -j DROP

#Create Logging Chain for accepted packets on OUTPUT CHAIN

iptables -N accept-output

#Rules for accept-output Chain

iptables -A accept-output -j LOG --log-prefix "OUTPUT-ACCEPTED"

iptables -A accept-output -j ACCEPT

#Create Logging Chain for dropped packets on OUTPUT CHAIN

iptables -N drop-output

#Rules for drop-output Chain

iptables -A drop-output -j LOG --log-prefix "OUTPUT-DROPPED"

iptables -A drop-output -j DROP

#Create Logging Chain for accepted packets on FORWARD CHAIN

iptables -N accept-forward

#Rules for accept-forward Chain

iptables -A accept-forward -j LOG --log-prefix "FORWARD-ACCEPTED"

iptables -A accept-forward -j ACCEPT

#Create Logging Chain for dropped packets on FORWARD CHAIN

iptables -N drop-forward

#Rules for drop-forward Chain

iptables -A drop-forward -j LOG --log-prefix "FORWARD-DROPPED"

iptables -A drop-forward -j DROP

#DNS

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 53 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 53 -m state --state ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p udp -s 172.16.20.64/26 --dport 53 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p udp -d 172.16.20.64/26 --sport 53 -m state --state ESTABLISHED,RELATED -j accept-forward

#DHCP

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

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

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

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

#Allow Apache

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 5151 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 5151 -m state --state ESTABLISHED,RELATED -j accept-forward

#Allow IIS

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 1515 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 1515 -m state --state ESTABLISHED,RELATED -j accept-forward

#Allow Traceroute

iptables -A INPUT -p icmp -j accept-input

iptables -A INPUT -p udp --dport 33434:33474 -j accept-input

iptables -A FORWARD -p icmp -j accept-forward

iptables -A FORWARD -p udp --dport 33343:33474 -j accept-forward

iptables -A OUTPUT -p icmp -j accept-output

iptables -A OUTPUT -p udp --dport 33434:33474 -j accept-output

#INPUT CHAIN RULES

iptables -A INPUT -j drop-input

#OUTPUT CHAIN RULES

iptables -A OUTPUT -j drop-output

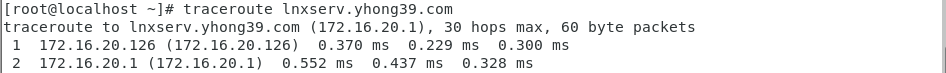
#FORWARD CHAIN RULES

iptables -A FORWARD -j drop-forward

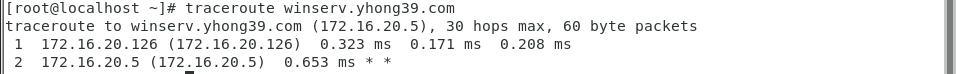
iptables -L -n

**Traceroute**

LinuxServer

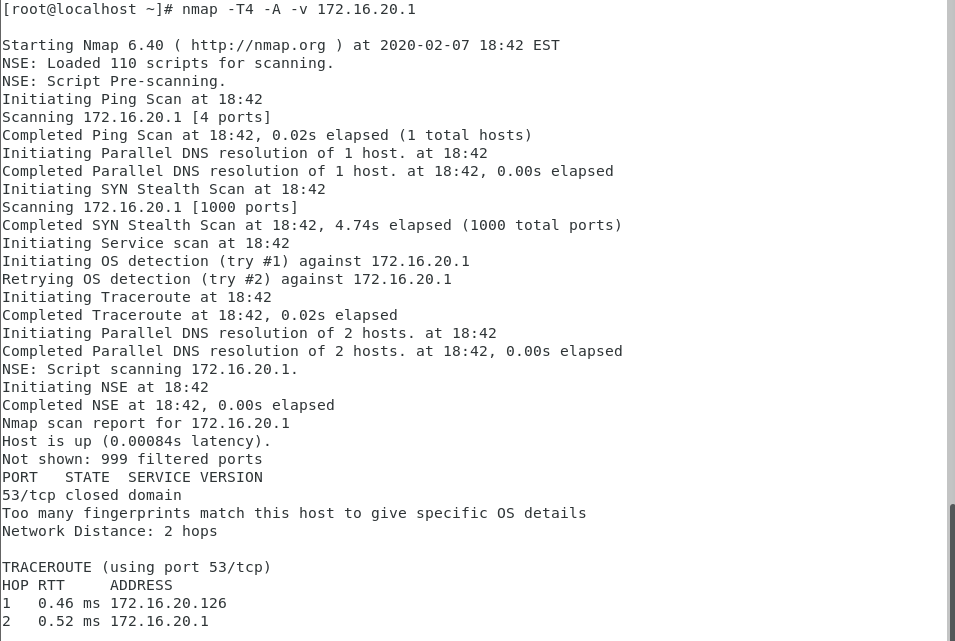


Winserv

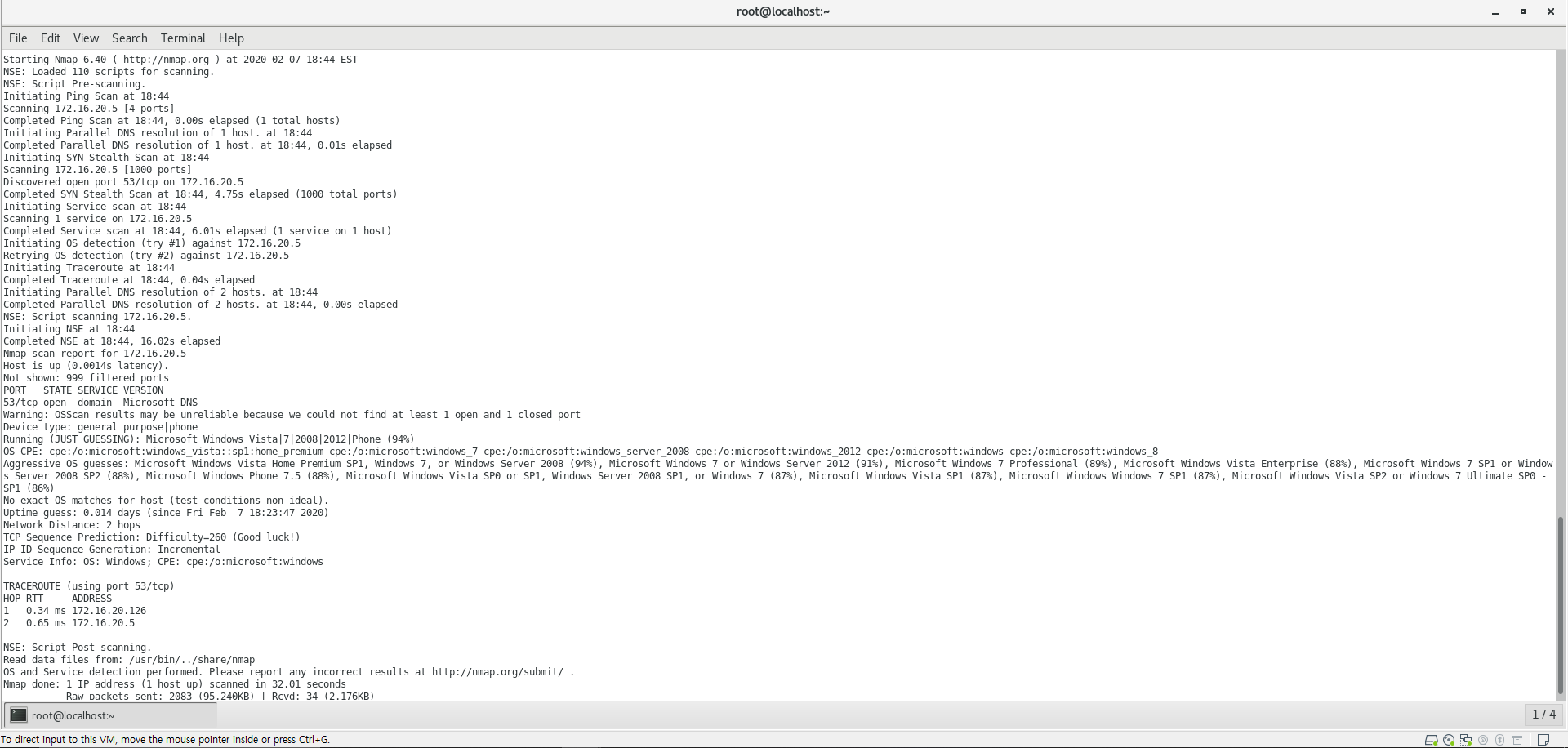


**Nmap service**

Nmap -T4 -A -v 172.16.20.1 (Linux Server)



Nmap -T4 -A -v 172.15.20.5 (Windows Server)

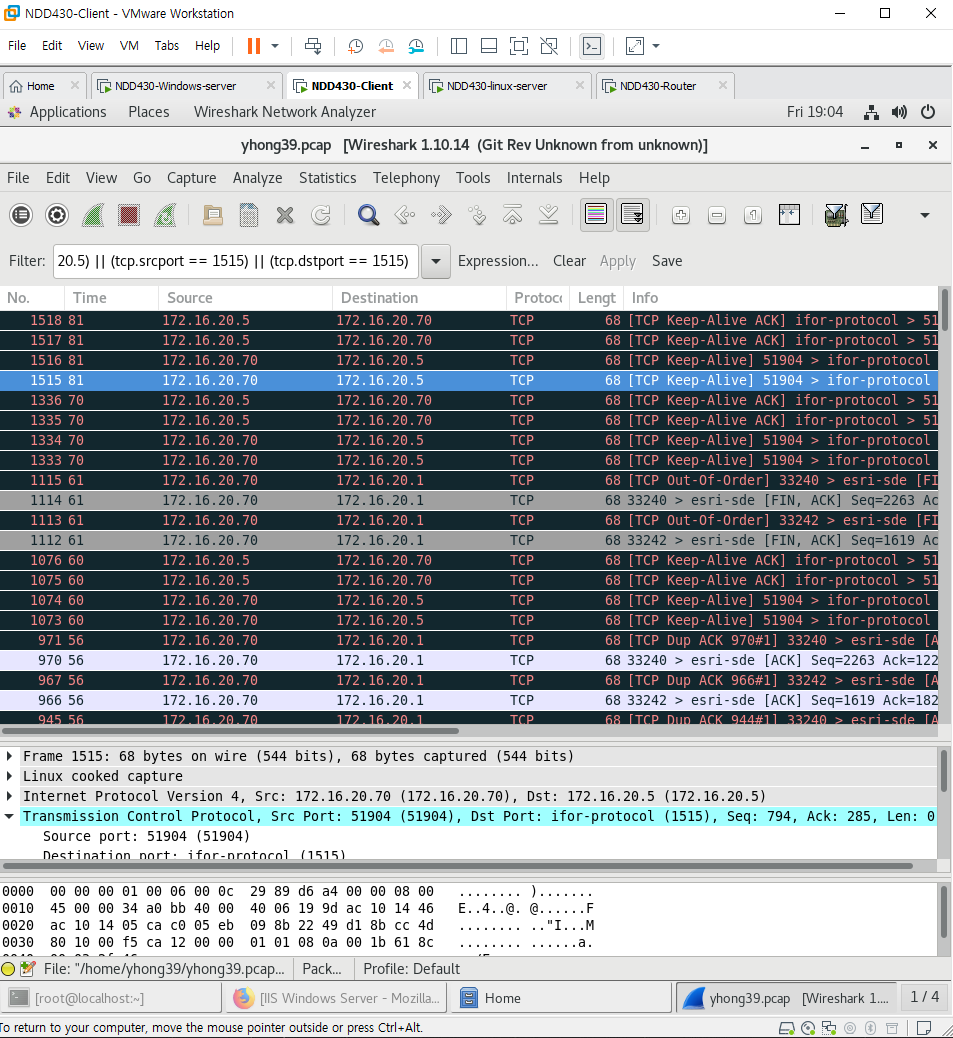


**Tcpdump**

Tcpdump -i any -w yhong39.pcap

Scp yhong39.pcap [root@172.16.20.70:/home/yhong39](mailto:root@172.16.20.70:/home/yhong39)

**(ip.src == 172.16.20.70) || (ip.dst == 172.16.20.5) || (tcp.srcport == 1515) || (tcp.dstport == 1515)**



**(ip.src == 172.16.20.70) || (ip.dst == 172.16.20.1) || (tcp.srcport == 5151) || (tcp.dstport == 5151)**

