**CheckPoint3**

**Windows Server**

**Filezilla**

Download filezilla <https://filezilla-project.org/download.php?type=server>

Installing by default.

Connect to server the default without password

Go to edit tab -> users -> add with password

Go setting tab -> passive mode settings -> user custom port range 20 – 21

**hMailserver**

download hmailserver <https://www.hmailserver.com/download>

Installing by default -> enter password

Domain -> add -> yhong39.com

Setting -> protocol -> Delivery of e-mail -> Local host name -> winserv.yhong39.com

Go -> DNS Manager -> Add MX record for winserv.yhong39.com

**Linux Server**

**MySQL**

Create user: create user ‘yhong39’@’172.16.20.70’ identified by ‘password’;

Privilege: Grant select on \*(table name).\*(database name) to yhong39@172.16.20.70;

**Client**

**Filezilla**

Host: winserv.yhong39.com -> Username and passwd: user1(created in windows filezilla) -> Port: 21

**Thunder Bird**

Add email -> Your name(Type full name) -> Email address(user1,2@yhong39.com) -> Password

Server hostname -> winserv.yhong39.com -> port 143(IMAP), port 25(SMTP) -> SSL(None) -> Authentication (Normal Password)

**MySQL**

Command - > mysql -u yhong39 -h lnxserv.yhong39.com -p

**SSH**

Ssh -p 5353 lnxserv.yhong39.com

Ssh -p 3535 172.16.20.126

**Router**

**Iptables**

**Scenario 1A**

#!/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

#SSH/SCP to Router

iptables -A INPUT -p tcp -s 172.16.20.64/26 --dport 3535 -m state --state NEW,ESTABLISHED,RELATED -j accept-input

iptables -A OUTPUT -p tcp -d 172.16.20.64/26 --sport 3535 -m state --state ESTABLISHED,RELATED -j accept-output

#SSH/SCP to Server

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 5353 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 5353 -m state --state ESTABLISHED,RELATED -j accept-forward

#HMAIL IMAP

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 143 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 143 -m state --state ESTABLISHED,RELATED -j accept-forward

#HMAIL SMTP

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 25 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 25 -m state --state ESTABLISHED,RELATED -j accept-forward

#FTP UNENCRYPTED

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 21 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 21 -m state --state ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 20 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 20 -m state --state ESTABLISHED,RELATED -j accept-forward

#MySQL

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 3306 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 3306 -m state --state ESTABLISHED,RELATED -j accept-forward

#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

**Scenario 1B**

#!/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

#SSH/SCP to Router

iptables -A INPUT -p tcp -s 172.16.20.64/26 --dport 3535 -m state --state NEW,ESTABLISHED,RELATED -j accept-input

iptables -A OUTPUT -p tcp -d 172.16.20.64/26 --sport 3535 -m state --state ESTABLISHED,RELATED -j accept-output

#SSH/SCP to Server

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 5353 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 5353 -m state --state ESTABLISHED,RELATED -j accept-forward

#HMAIL IMAP

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 143 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 143 -m state --state ESTABLISHED,RELATED -j accept-forward

#HMAIL SMTP

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 25 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 25 -m state --state ESTABLISHED,RELATED -j accept-forward

#FTP UNENCRYPTED

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 21 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 21 -m state --state ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 20 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 20 -m state --state ESTABLISHED,RELATED -j accept-forward

#MySQL

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 3306 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 3306 -m state --state ESTABLISHED,RELATED -j accept-forward

#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

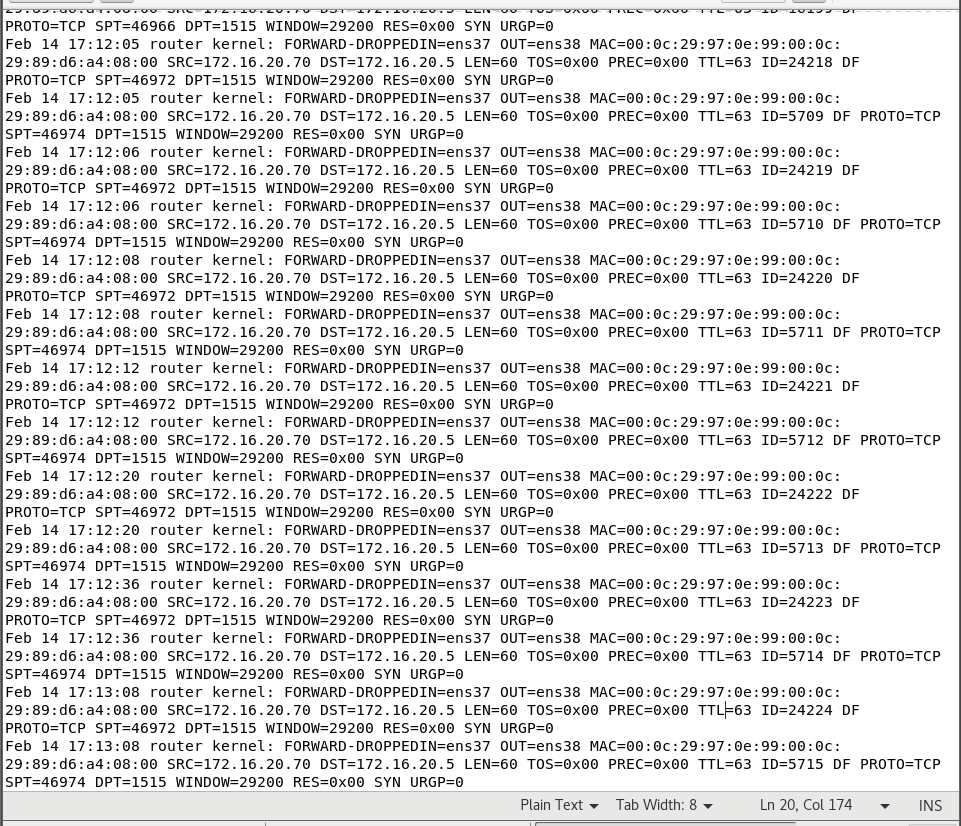
#FORWARD CHAIN RULES

iptables -A FORWARD -j drop-forward

iptables -L -n

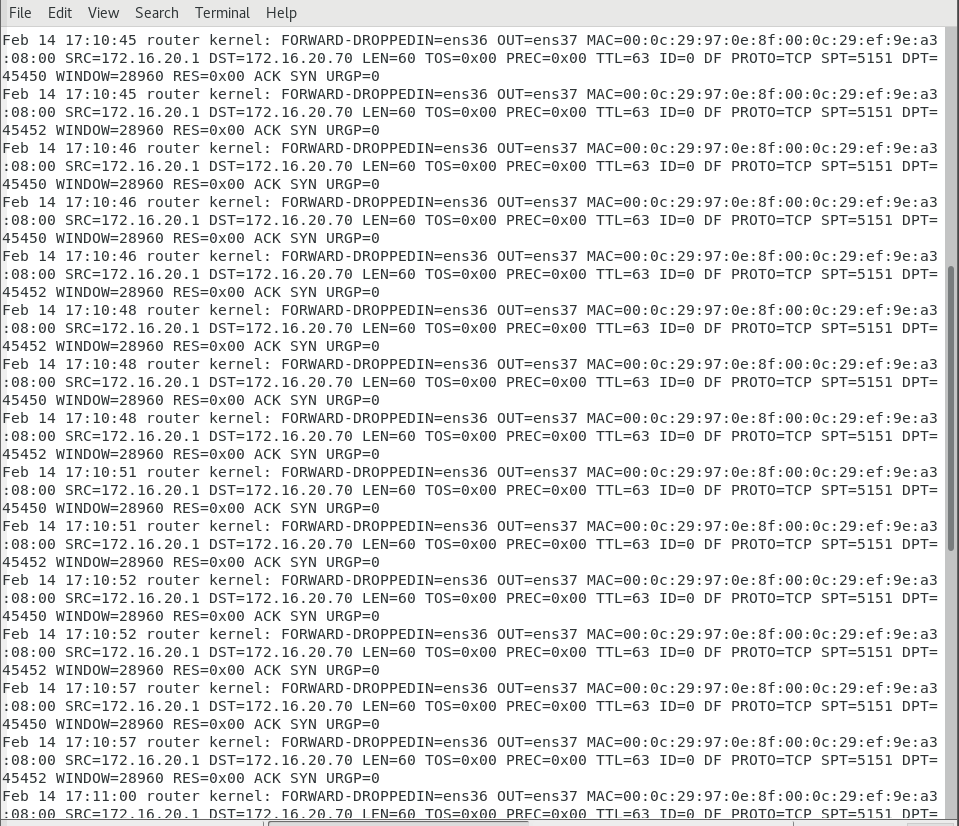
**A dropped request** from your client to your IIS server

Cat /var/log/message | grep “SRC = 172.16.20.70”



**A dropped response** from your Apache server to your client

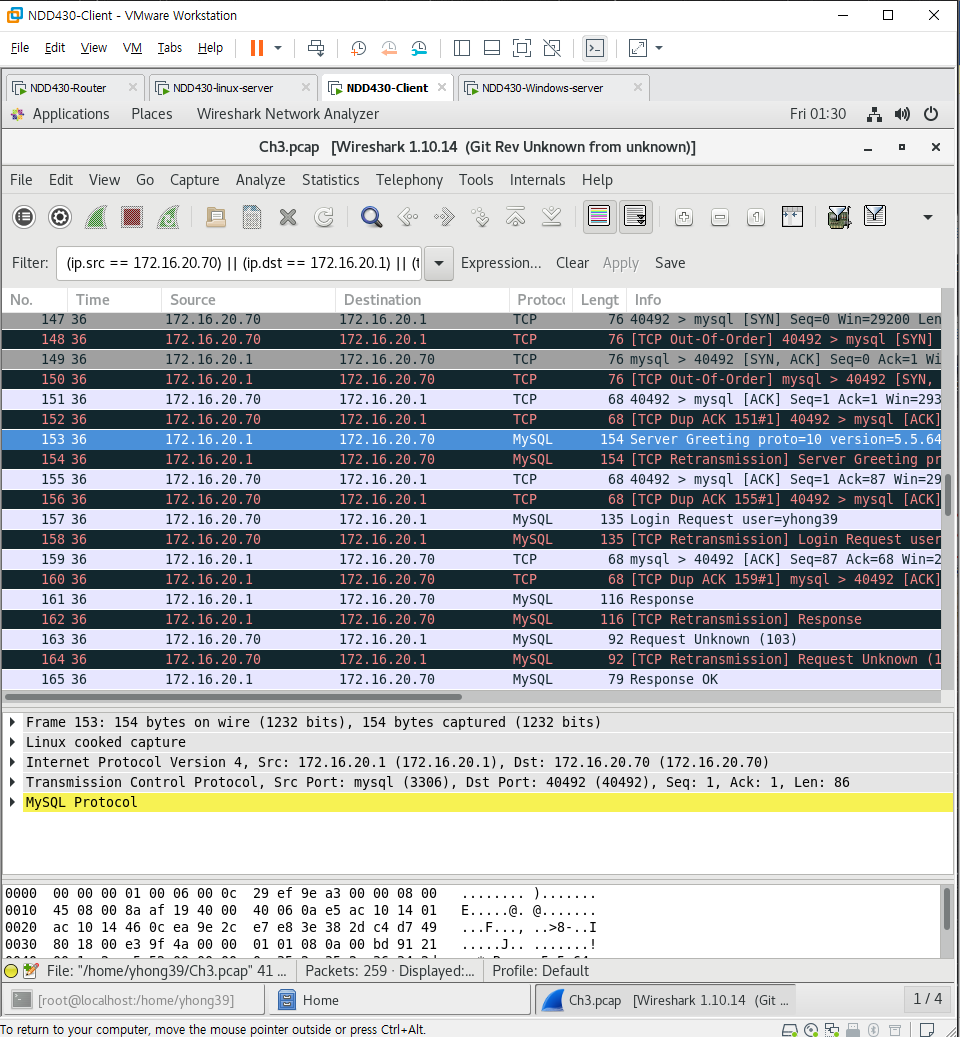
Cat /var/log/message | grep “SRC=172.16.20.1”



**Tcpdump Capture**

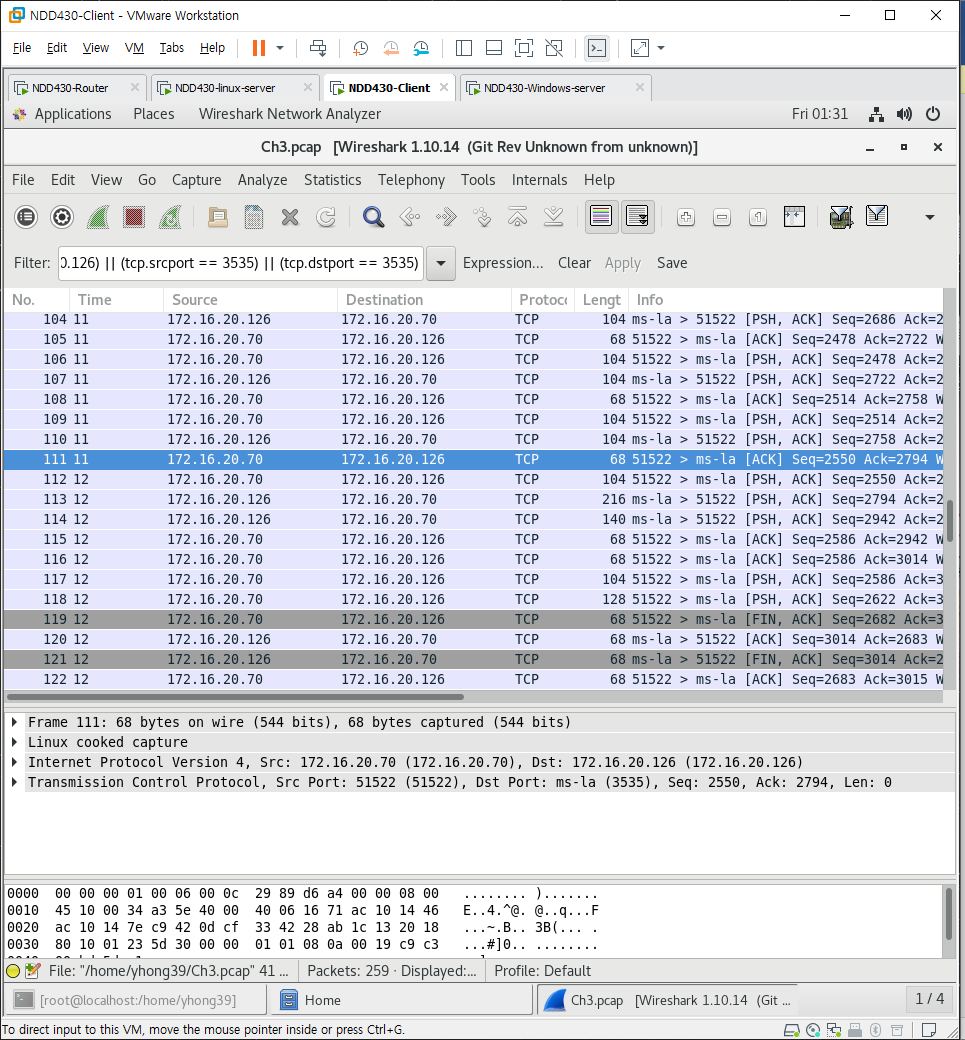
Tcpdump -I any -w ch3.pcap -> Scp ch3.pcap 172.16.20.70:/home/yhong39

(ip.src == 172.16.20.70) || (ip.dst == 172.16.20.1) || (tcp.srcport == 3306) || (tcp.dstport == 3306) MysqlCapture



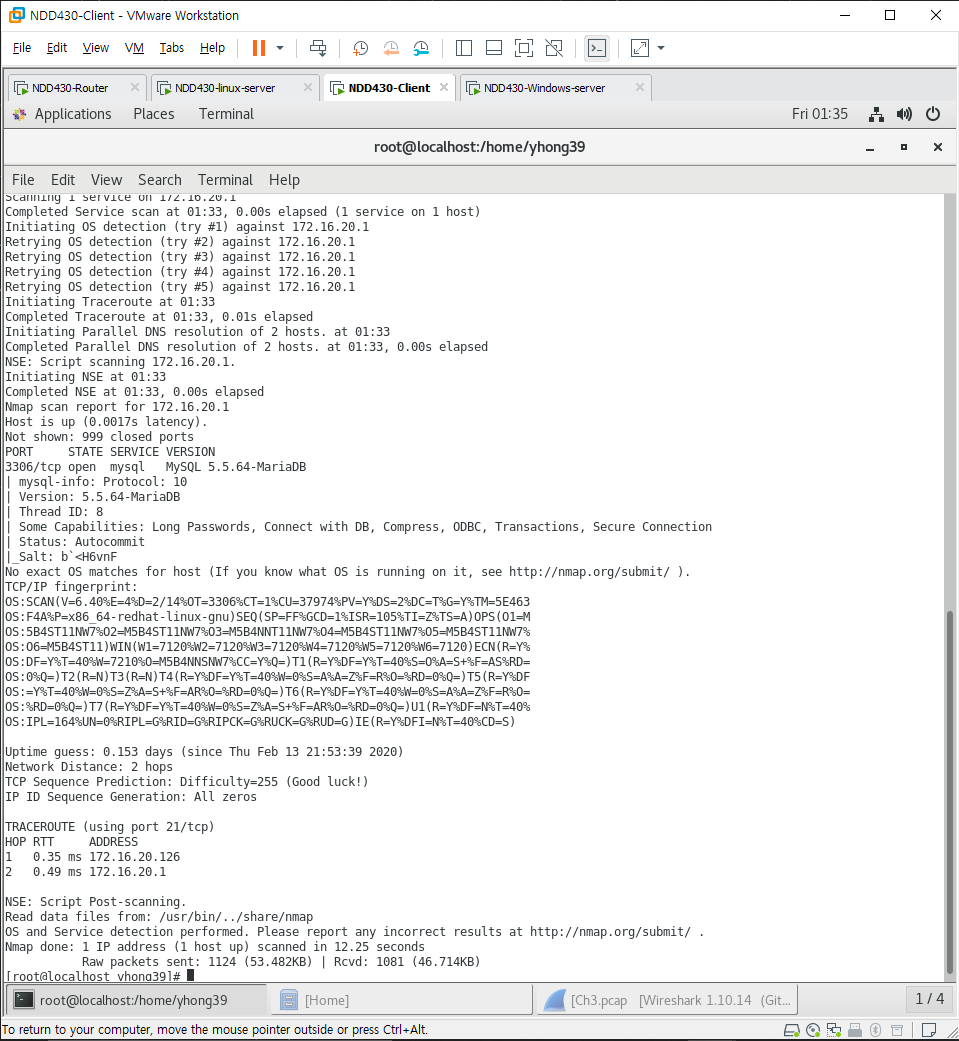
sshCapture

(ip.src == 172.16.20.70) || (ip.dst == 172.16.20.126) || (tcp.srcport == 3535) || (tcp.dstport == 3535)



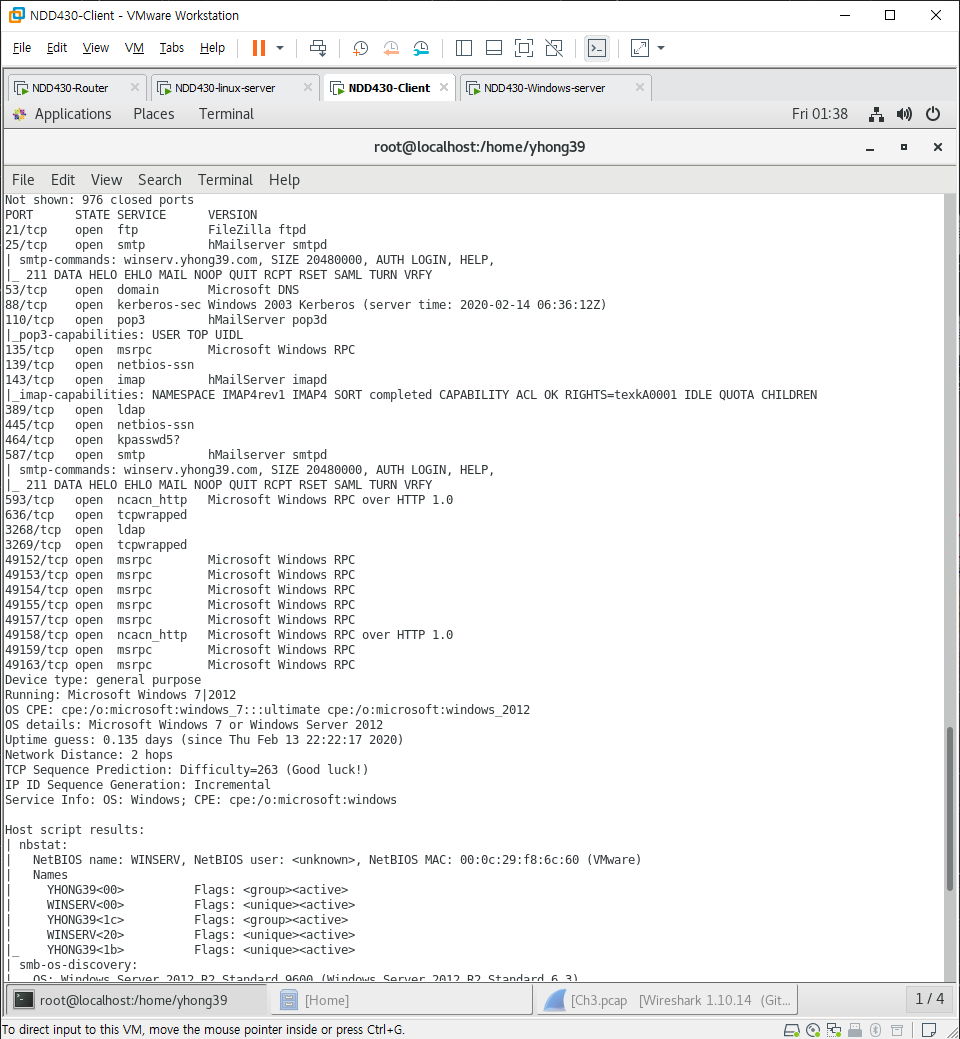
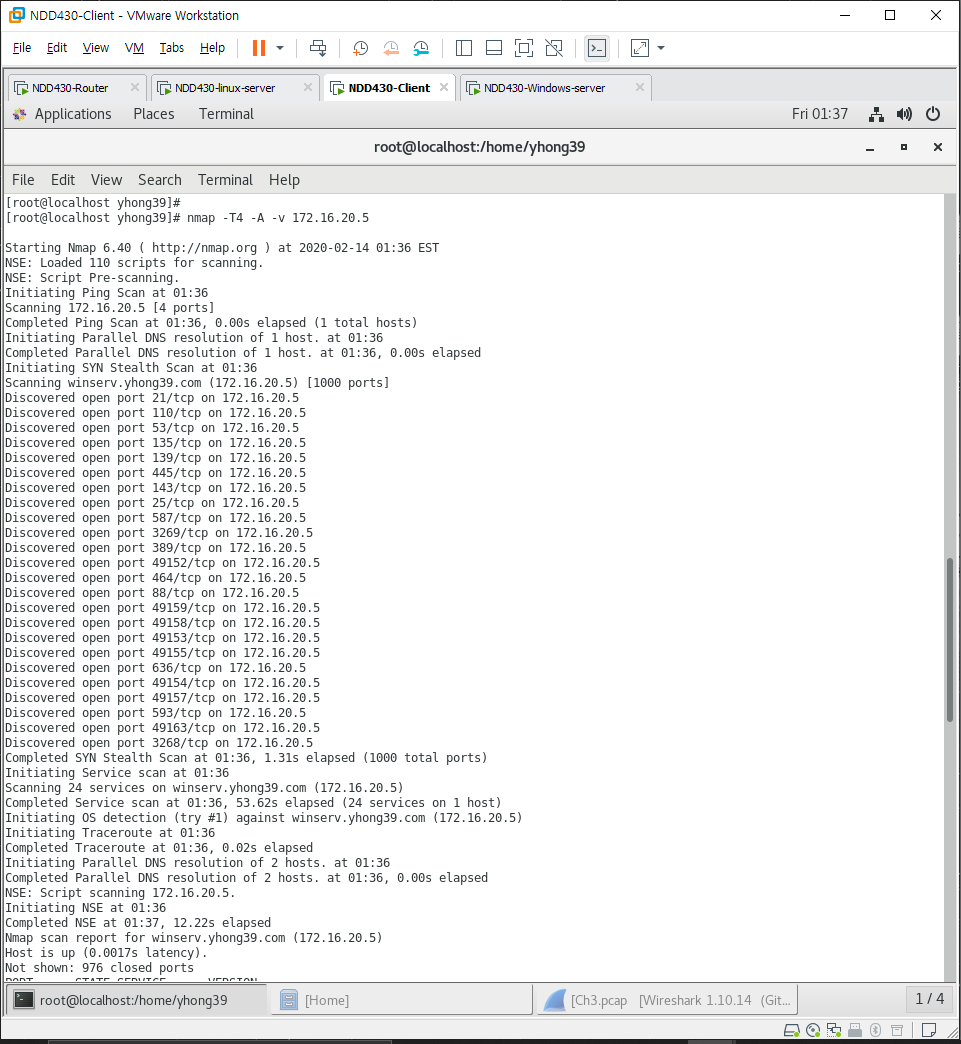
**NmapToLnx**

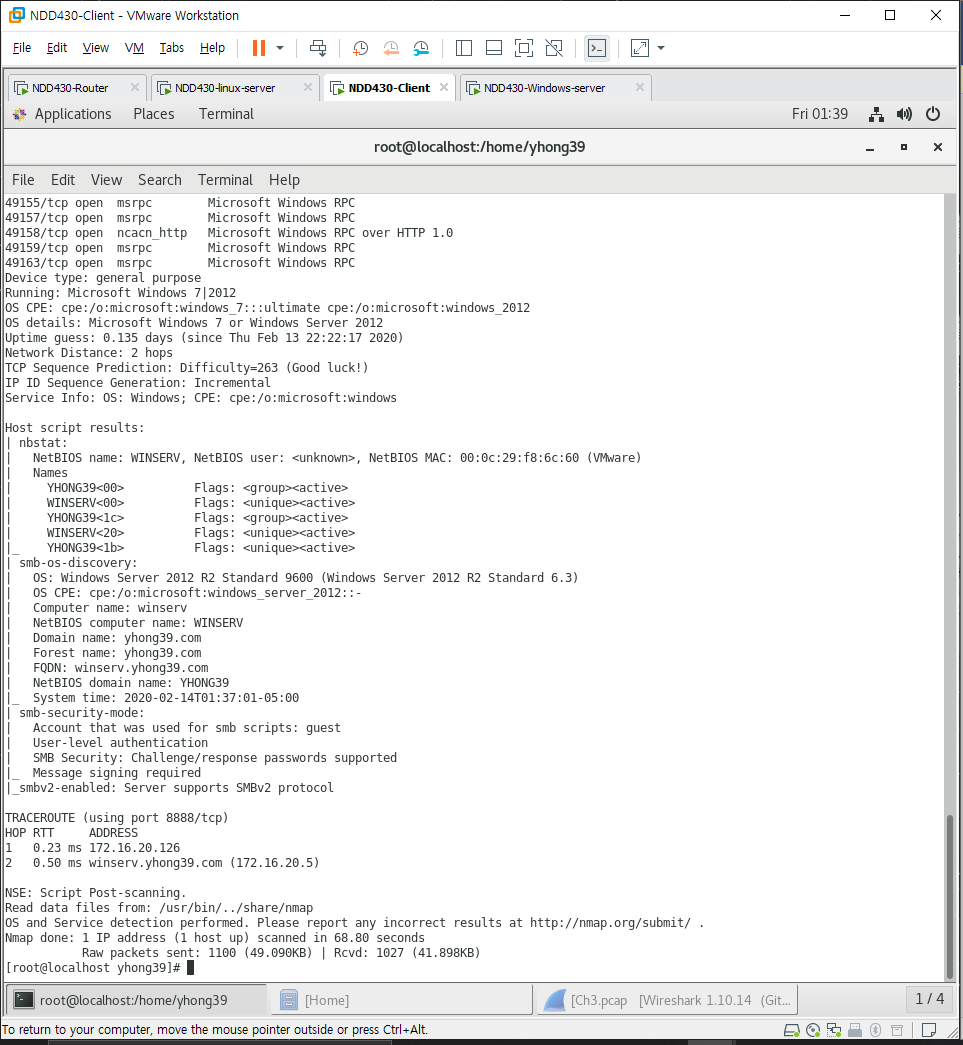
nmap -T4 -A -v 172.16.20.1



**NmapToWin**

nmap -T4 -A -v 172.16.20.5





<https://peemangit.tistory.com/54>