

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 33434:33474 -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 33434:33474 -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
```

```
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"
```

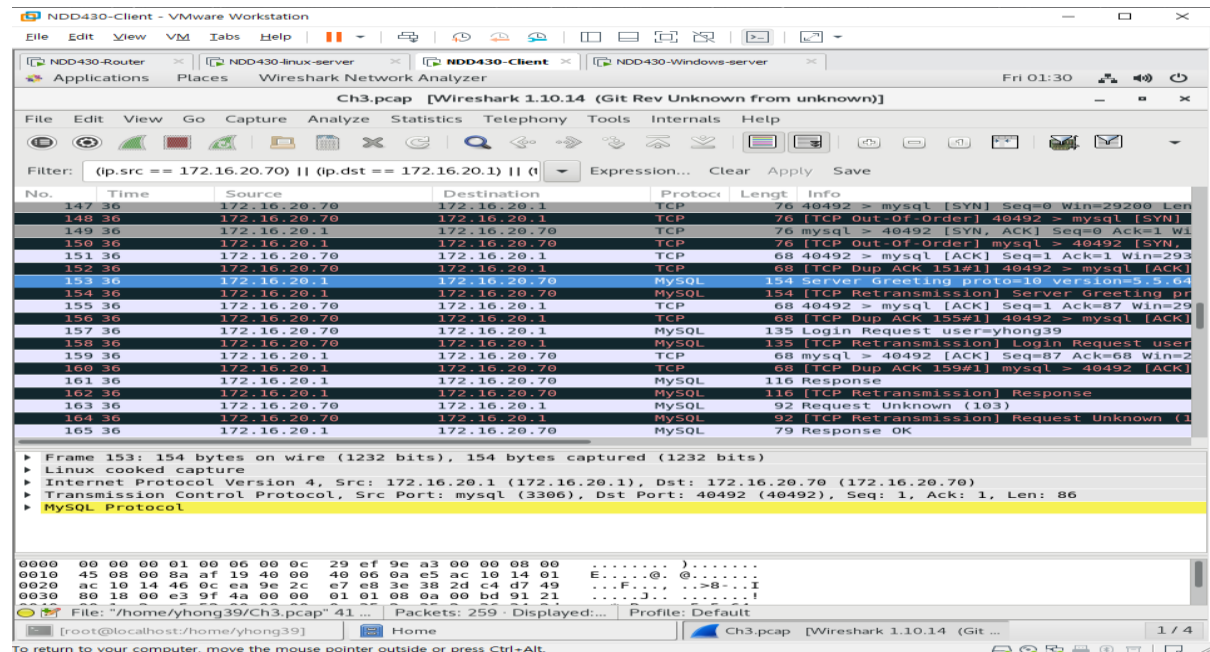
[illegible]

Tcpdump Capture

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

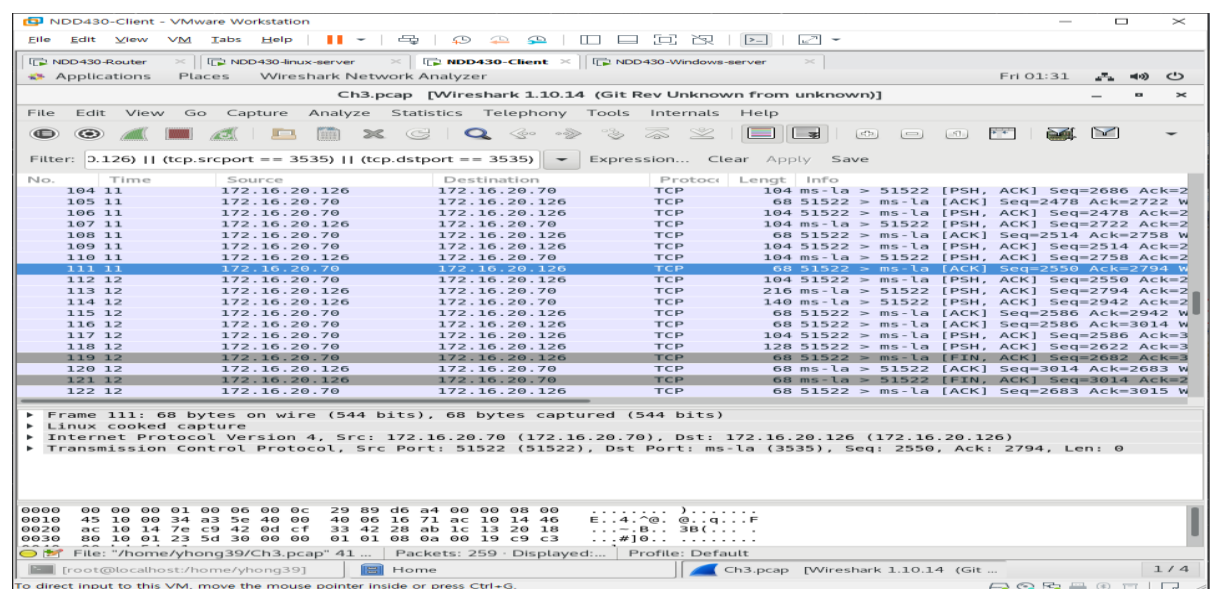
(ip.src == 172.16.20.70) || (ip.dst == 172.16.20.1) || (tcp.srcport == 3306) || (tcp.dstport == 3306)

MySQLCapture



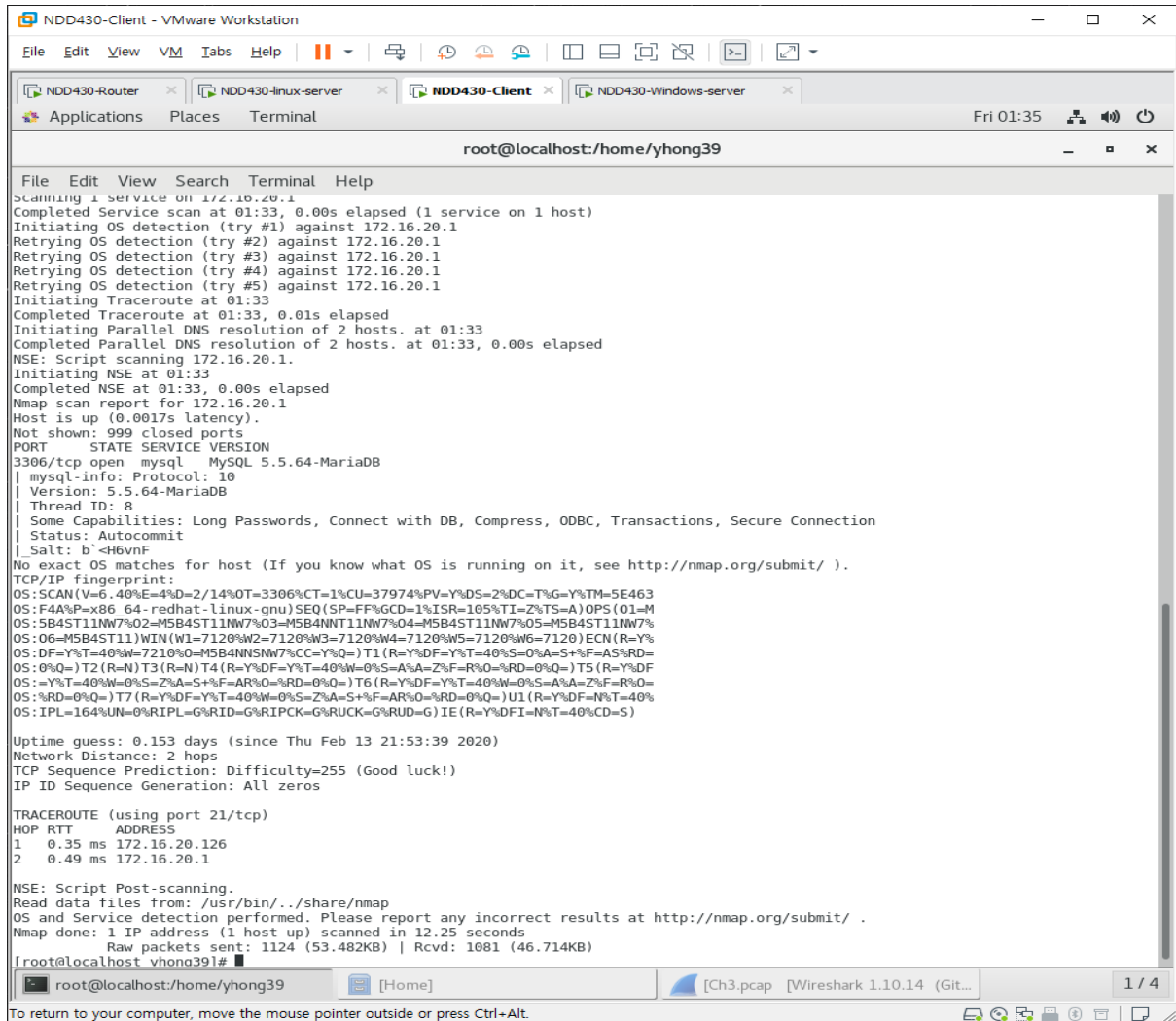
sshCapture

(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



```
root@localhost:/home/yhong39
File Edit View Search Terminal Help
Scanning 1 service on 172.16.20.1
Completed Service scan at 01:33, 0.00s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 172.16.20.1
Retrying OS detection (try #2) against 172.16.20.1
Retrying OS detection (try #3) against 172.16.20.1
Retrying OS detection (try #4) against 172.16.20.1
Retrying OS detection (try #5) against 172.16.20.1
Initiating Traceroute at 01:33
Completed Traceroute at 01:33, 0.01s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 01:33
Completed Parallel DNS resolution of 2 hosts. at 01:33, 0.00s elapsed
NSE: Script scanning 172.16.20.1.
Initiating NSE at 01:33
Completed NSE at 01:33, 0.00s elapsed
Nmap scan report for 172.16.20.1
Host is up (0.0017s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql   MySQL 5.5.64-MariaDB
|_ mysql-info: Protocol: 10
|_ Version: 5.5.64-MariaDB
|_ Thread ID: 8
|_ Some Capabilities: Long Passwords, Connect with DB, Compress, ODBC, Transactions, Secure Connection
|_ Status: Autocommit
|_ Salt: b'<H6vnF
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS: SCAN(V=6.40%E=4%D=2/14%OT=3306%CT=1%CU=37974%PV=Y%DS=2%DC=T%G=Y%TM=5E463
OS: F4A%P=x86_64-redhat-linux-gnu)SEQ(SP=FF%GCD=1%ISR=105%TI=Z%TS=A)OPS(O1=M
OS: 5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%
OS: O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%
OS: DF=Y%T=40%W=7210%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=
OS: 0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=0%RD=0%Q=)T5(R=Y%DF
OS: =Y%T=40%W=0%S=Z%A=S+%F=AR%O=0%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=
OS: %RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=0%RD=0%Q=)U1(R=Y%DF=N%T=40%
OS: IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

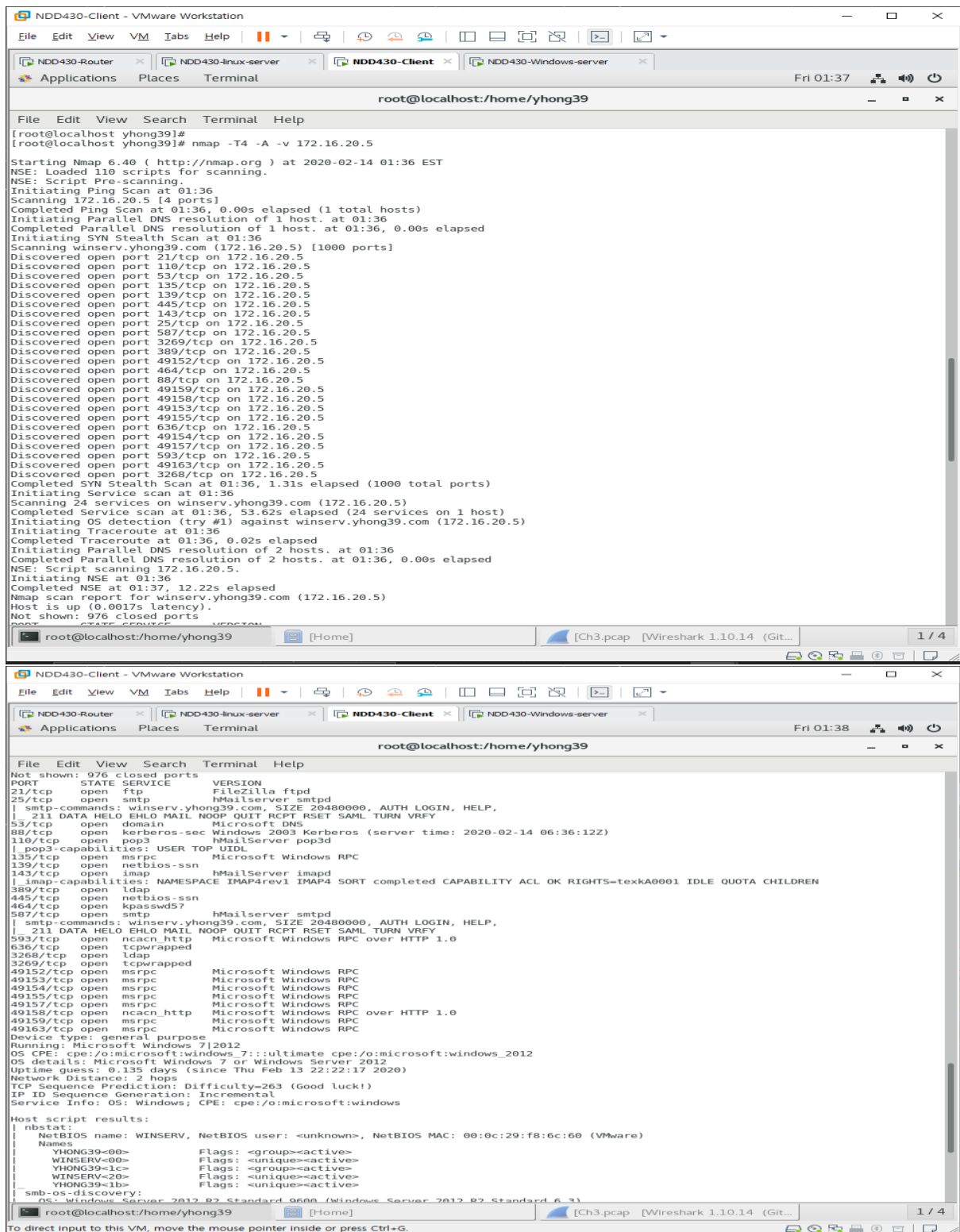
Uptime guess: 0.153 days (since Thu Feb 13 21:53:39 2020)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 21/tcp)
HOP RTT ADDRESS
1 0.35 ms 172.16.20.126
2 0.49 ms 172.16.20.1

NSE: Script Post-scanning.
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.25 seconds
Raw packets sent: 1124 (53.482KB) | Rcvd: 1081 (46.714KB)
root@localhost yhong39#
```


NmapToWin

nmap -T4 -A -v 172.16.20.5



The screenshot displays a VMware Workstation interface with a terminal window titled "root@localhost:/home/yhong39". The terminal shows the execution of the command `nmap -T4 -A -v 172.16.20.5`. The output is a detailed Nmap scan report for the host 172.16.20.5, which is identified as winserv.yhong39.com. The scan includes a SYN Stealth Scan, a Service scan, and an OS detection attempt. The report lists 24 open ports, including 21/tcp (FileZilla ftpd), 25/tcp (hMailserver smtpd), 139/tcp (Microsoft Windows RPC), and 445/tcp (Microsoft Windows RPC). The OS is identified as Microsoft Windows 7|2012. The terminal window is part of a larger VMware interface showing other virtual machines like NDD430-Router, NDD430-linux-server, and NDD430-Windows-server.

```
root@localhost:/home/yhong39# nmap -T4 -A -v 172.16.20.5
Starting Nmap 6.40 ( http://nmap.org ) at 2020-02-14 01:36 EST
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 01:36
Scanning 172.16.20.5 [4 ports]
Completed Ping Scan at 01:36, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:36
Completed Parallel DNS resolution of 1 host. at 01:36, 0.00s elapsed
Initiating SYN Stealth Scan at 01:36
Scanning winserv.yhong39.com (172.16.20.5) [1000 ports]
Discovered open port 21/tcp on 172.16.20.5
Discovered open port 110/tcp on 172.16.20.5
Discovered open port 53/tcp on 172.16.20.5
Discovered open port 135/tcp on 172.16.20.5
Discovered open port 139/tcp on 172.16.20.5
Discovered open port 445/tcp on 172.16.20.5
Discovered open port 143/tcp on 172.16.20.5
Discovered open port 25/tcp on 172.16.20.5
Discovered open port 587/tcp on 172.16.20.5
Discovered open port 3269/tcp on 172.16.20.5
Discovered open port 389/tcp on 172.16.20.5
Discovered open port 49152/tcp on 172.16.20.5
Discovered open port 464/tcp on 172.16.20.5
Discovered open port 88/tcp on 172.16.20.5
Discovered open port 49159/tcp on 172.16.20.5
Discovered open port 49158/tcp on 172.16.20.5
Discovered open port 49153/tcp on 172.16.20.5
Discovered open port 49155/tcp on 172.16.20.5
Discovered open port 636/tcp on 172.16.20.5
Discovered open port 49154/tcp on 172.16.20.5
Discovered open port 49157/tcp on 172.16.20.5
Discovered open port 593/tcp on 172.16.20.5
Discovered open port 49163/tcp on 172.16.20.5
Discovered open port 3268/tcp on 172.16.20.5
Completed SYN Stealth Scan at 01:36, 1.31s elapsed (1000 total ports)
Initiating Service scan at 01:36
Scanning 24 services on winserv.yhong39.com (172.16.20.5)
Completed Service scan at 01:36, 53.62s elapsed (24 services on 1 host)
Initiating OS detection (try #1) against winserv.yhong39.com (172.16.20.5)
Initiating Traceroute at 01:36
Completed Traceroute at 01:36, 0.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 01:36
Completed Parallel DNS resolution of 2 hosts. at 01:36, 0.00s elapsed
NSE: Script scanning 172.16.20.5.
Initiating NSE at 01:36
Completed NSE at 01:37, 12.22s elapsed
Nmap scan report for winserv.yhong39.com (172.16.20.5)
Host is up (0.0017s latency).
Not shown: 976 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
| smtp_commands: winserv.yhong39.com, SIZE 20480000, AUTH LOGIN, HELP,
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
53/tcp    open  domain
88/tcp    open  kerberos-sec
110/tcp   open  pop3
|_ pop3_capabilities: USER TOP UIDL
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
| imap_capabilities: NAMESPACE IMAP4rev1 IMAP4 SORT completed CAPABILITY ACL OK RIGHTS=texka0001 IDLE QUOTA CHILDREN
389/tcp   open  ldap
445/tcp   open  netbios-ssn
464/tcp   open  kpasswd5?
587/tcp   open  smtp
| smtp_commands: winserv.yhong39.com, SIZE 20480000, AUTH LOGIN, HELP,
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
593/tcp   open  ncacn_http
636/tcp   open  tcpwrapped
3268/tcp  open  ldap
3269/tcp  open  tcpwrapped
49152/tcp open  msrpc
49153/tcp open  msrpc
49154/tcp open  msrpc
49155/tcp open  msrpc
49157/tcp open  msrpc
49158/tcp open  ncacn_http
49159/tcp open  msrpc
49163/tcp open  msrpc
Device type: general purpose
Running: Microsoft Windows 7|2012
OS CPE: cpe:/o:microsoft:windows_7::ultimate cpe:/o:microsoft:windows_2012
OS details: Microsoft Windows 7 or Windows Server 2012
Uptime guess: 0.135 days (since Thu Feb 13 22:22:17 2020)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ nbstat:
|_ NetBIOS name: WINSERV, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:f8:6c:60 (VMware)
|_ Names:
|_ YHONG39-00> Flags: <group><active>
|_ WINSERV-00> Flags: <unique><active>
|_ YHONG39-1c> Flags: <group><active>
|_ WINSERV-20> Flags: <unique><active>
|_ YHONG39-1b> Flags: <unique><active>
|_ smb-os-discovery:
|_ OS: Windows Server 2012 R2 Standard 6500 (Windows Server 2012 R2 Standard 6.3)
```

```
NDD430-Client - VMware Workstation
File Edit View VM Tabs Help
NDD430-Router x NDD430-linux-server x NDD430-Client x NDD430-Windows-server x
Applications Places Terminal
Fri 01:39
root@localhost:/home/yhong39

File Edit View Search Terminal Help
49155/tcp open msrpc Microsoft Windows RPC
49157/tcp open msrpc Microsoft Windows RPC
49158/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
49159/tcp open msrpc Microsoft Windows RPC
49163/tcp open msrpc Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows 7|2012
OS CPE: cpe:/o:microsoft:windows_7::ultimate cpe:/o:microsoft:windows_2012
OS details: Microsoft Windows 7 or Windows Server 2012
Uptime guess: 0.135 days (since Thu Feb 13 22:22:17 2020)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat:
| NetBIOS name: WINSERV, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:f8:6c:60 (VMware)
| Names
| YHONG39<00> Flags: <group><active>
| WINSERV<00> Flags: <unique><active>
| YHONG39<1c> Flags: <group><active>
| WINSERV<20> Flags: <unique><active>
| YHONG39<1b> Flags: <unique><active>
|_
| smb-os-discovery:
| OS: Windows Server 2012 R2 Standard 9600 (Windows Server 2012 R2 Standard 6.3)
| OS CPE: cpe:/o:microsoft:windows_server_2012:-
| Computer name: winserv
| NetBIOS computer name: WINSERV
| Domain name: yhong39.com
| Forest name: yhong39.com
| FQDN: winserv.yhong39.com
| NetBIOS domain name: YHONG39
|_ System time: 2020-02-14T01:37:01-05:00
|_ smb-security-mode:
| Account that was used for smb scripts: guest
| User-level authentication
| SMB Security: Challenge/response passwords supported
|_ Message signing required
|_ smb-v2-enabled: Server supports SMBv2 protocol

TRACEROUTE (using port 8888/tcp)
HOP RTT ADDRESS
1 0.23 ms 172.16.20.126
2 0.50 ms winserv.yhong39.com (172.16.20.5)

NSE: Script Post-scanning.
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 68.80 seconds
Raw packets sent: 1100 (49.090KB) | Rcvd: 1027 (41.898KB)
[root@localhost yhong39]#
```

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