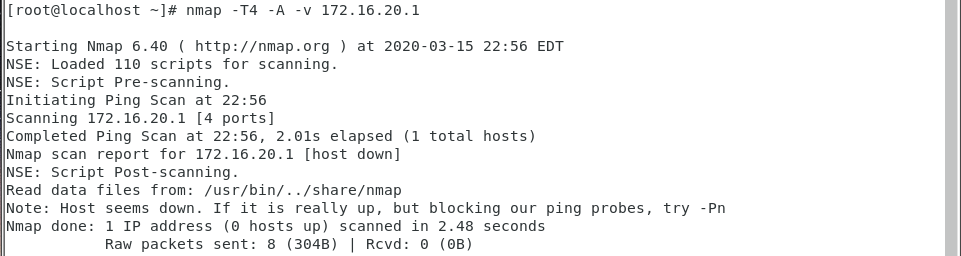
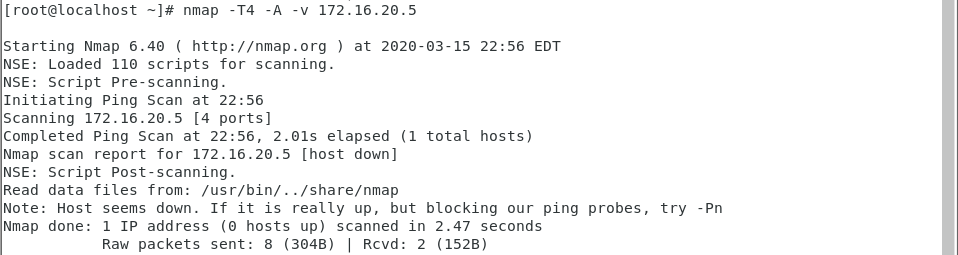
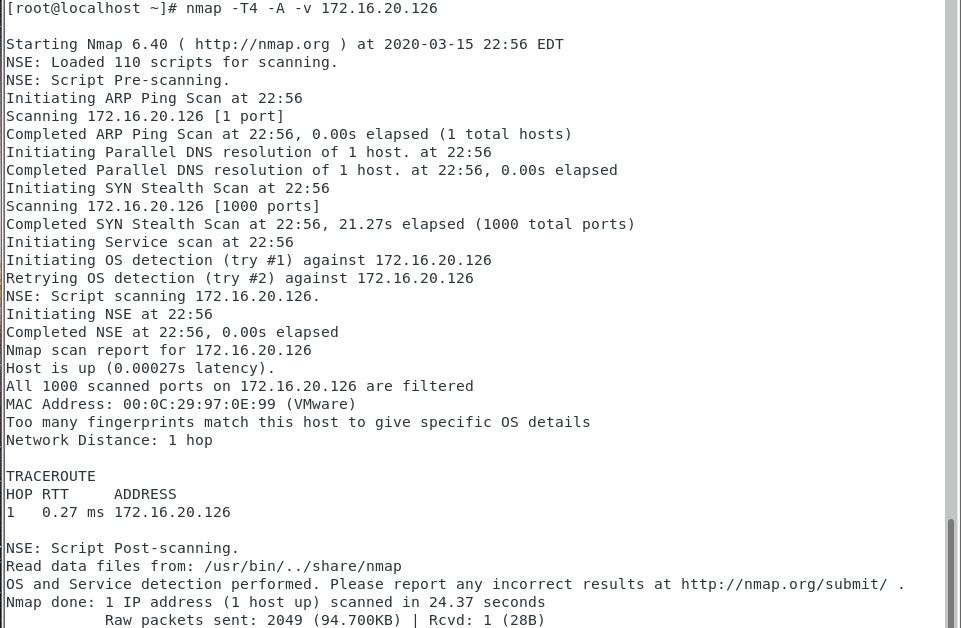
**Scenario 2**







#!/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

#Create logging Chain for dropped inbound packets on DROP-INBOUND CHAIN

iptables -N drop-inbound

#Rules for drop-inbound chain

iptables -A drop-inbound -j LOG --log-prefix "DROPPED-INBOUND"

iptables -A drop-inbound -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 drop-inbound

#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 drop-inbound

#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 drop-inbound

#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 drop-inbound

#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 drop-inbound

#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 drop-inbound

#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 drop-inbound

iptables -A FORWARD -p udp --dport 33343:33474 -j drop-inbound

#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

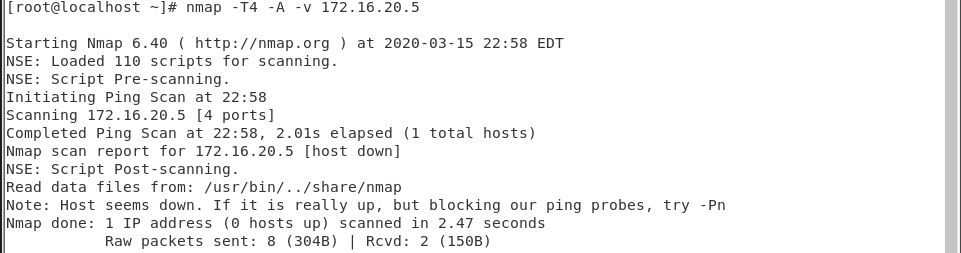
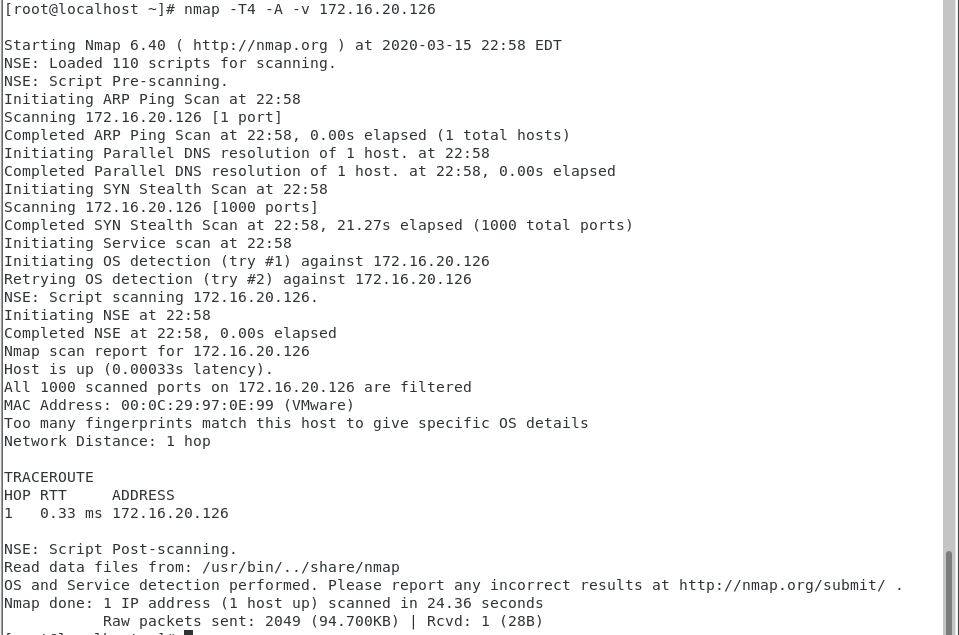
#FORWARD CHAIN RULES

iptables -A FORWARD -j drop-forward

iptables -L -n

**Scenario 3**

****

’

!/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

#Create logging Chain for dropped inbound packets on DROP-INBOUND CHAIN

iptables -N drop-inbound

#Rules for drop-inbound chain

iptables -A drop-inbound -j LOG --log-prefix "DROPPED-INBOUND"

iptables -A drop-inbound -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 drop-inbound

#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 drop-inbound

#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 drop-inbound

#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 drop-inbound

#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 drop-inbound

#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 drop-inbound

#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 drop-inbound

#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 drop-inbound

#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 drop-inbound

iptables -A FORWARD -p udp --dport 33343:33474 -j drop-inbound

#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

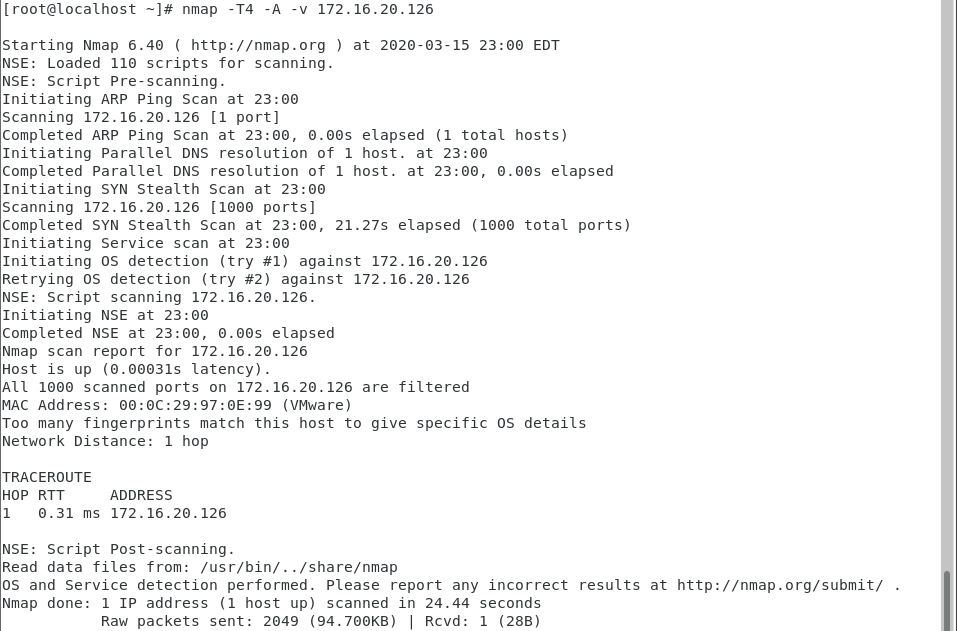
iptables -A FORWARD -j drop-forward

iptables -L -n

**Scenario 4**

****





#!/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

#Create Logging Chain for dropped inbound packets on DROP-OUTBOUND CHAIN

iptables -N drop-outbound

#Rules for drop-outbound chain

iptables -A drop-outbound -j LOG --log-prefix "DROPPED-OUTBOUND"

iptables -A drop-outbound -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 drop-inbound

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

#HMAIL SMTP

#iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 25 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

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

#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 drop-inbound

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

#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 drop-inbound

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

#Allow IIS

#iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 1515 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

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

#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 drop-outbound

iptables -A FORWARD -p udp --dport 33343:33474 -j drop-outbound

#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

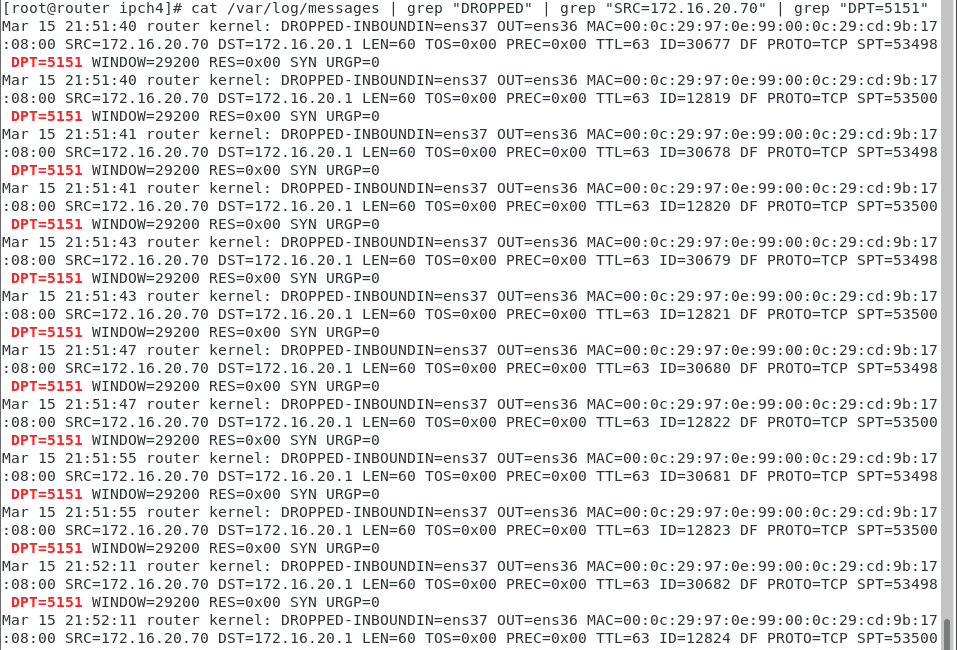
iptables -A FORWARD -j drop-forward

iptables -L -n

**Logging**

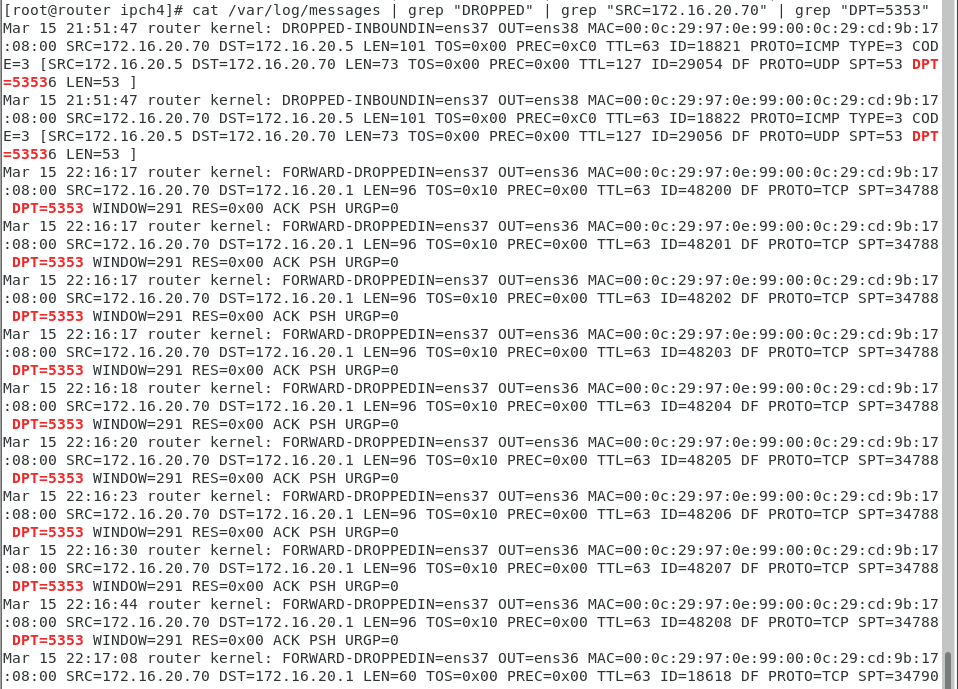
Cat /var/log/messages

A DROPPED APACHE request from you Client



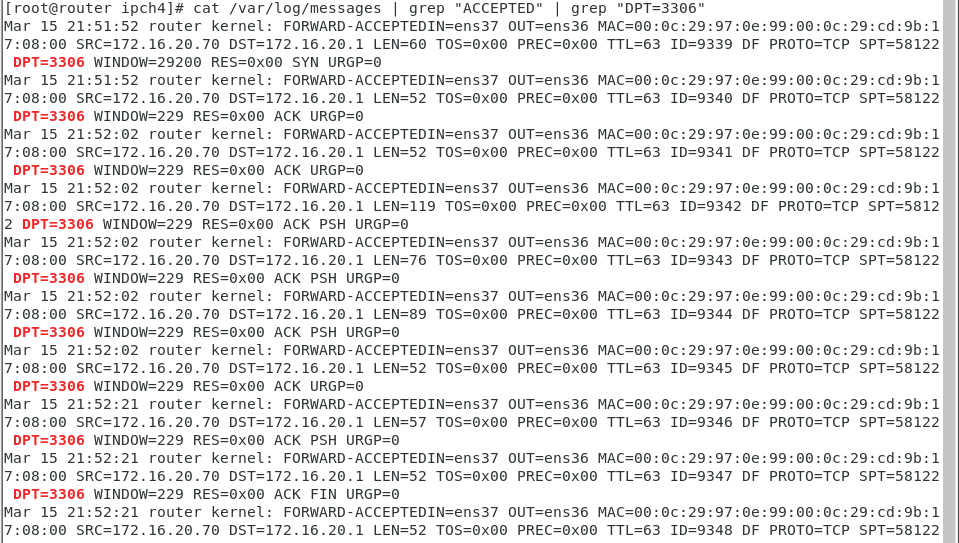
A DROPPED APACHE response from your Linux Server

A DROPPED SSH request to your LINUX Server

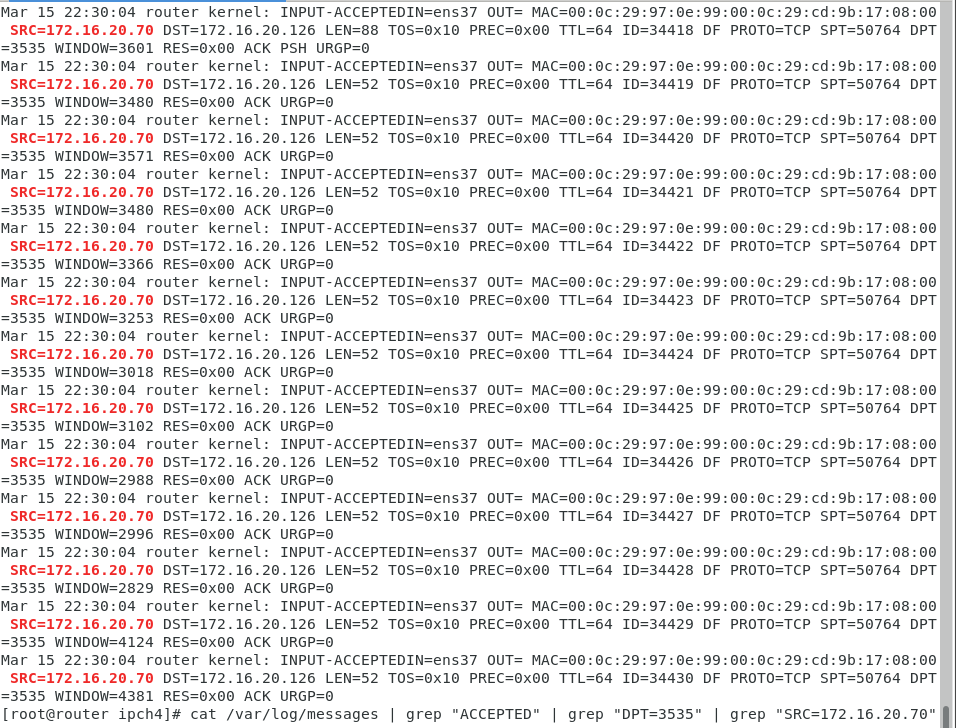
* 

A DROPPED IMAP response from your Windows Server

AN ACCEPTED MYSQL request from your Client



AN ACCEPTED SSH request to your router



AN ACCEPTED FTP response from your Windows Server (Port 20)

