A Basic Iptables Firewall

Alexander M. Hendren

Nova Scotia Community College, Cyber Security

ISEC2022

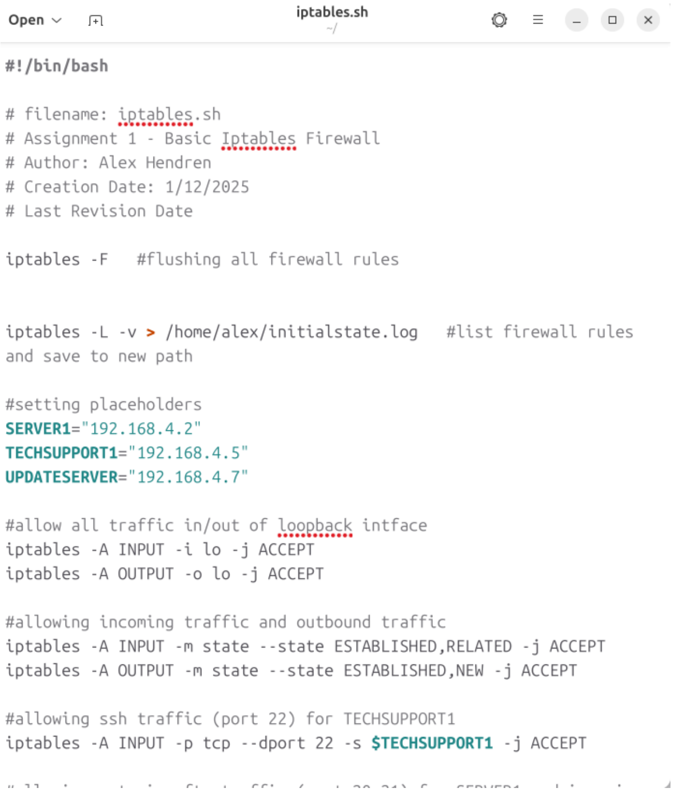
Assignment 1

January 13th, 2025

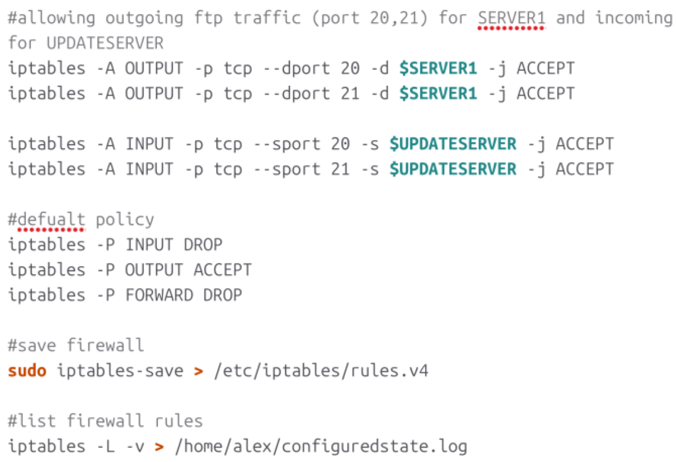
Table of Contents

Iptables Firewall Script

In this section, I have created a Linux script that is a basic iptables firewall.



```
#!/bin/bash

# filename: iptables.sh
# Assignment 1 - Basic Iptables Firewall
# Author: Alex Hendren
# Creation Date: 1/12/2025
# Last Revision Date

iptables -F   #flushing all firewall rules


iptables -L -v > /home/alex/initialstate.log   #list firewall rules
and save to new path

#setting placeholders
SERVER1="192.168.4.2"
TECHSUPPORT1="192.168.4.5"
UPDATESERVER="192.168.4.7"

#allow all traffic in/out of loopback intface
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

#allowing incoming traffic and outbound traffic
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,NEW -j ACCEPT

#allowing ssh traffic (port 22) for TECHSUPPORT1
iptables -A INPUT -p tcp --dport 22 -s $TECHSUPPORT1 -j ACCEPT
```

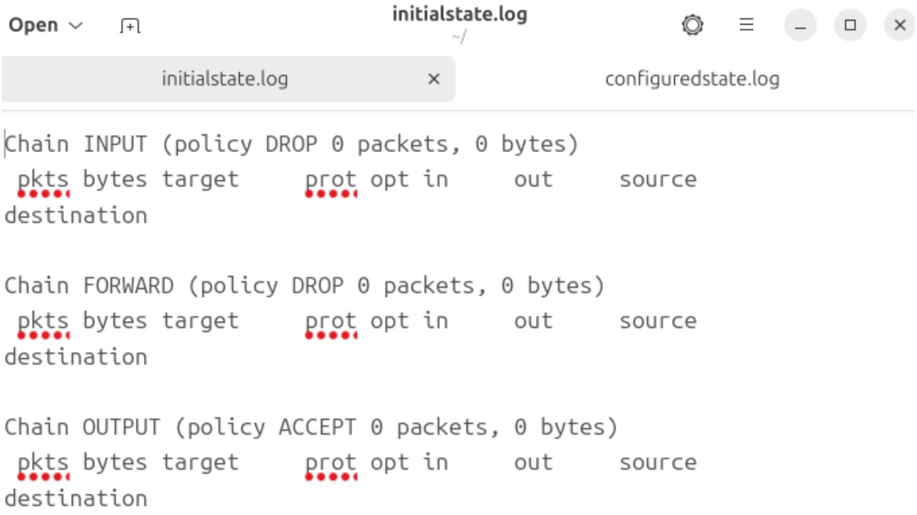


```
#allowing outgoing ftp traffic (port 20,21) for SERVER1 and incoming
for UPDATESERVER
iptables -A OUTPUT -p tcp --dport 20 -d $SERVER1 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 21 -d $SERVER1 -j ACCEPT

iptables -A INPUT -p tcp --sport 20 -s $UPDATESERVER -j ACCEPT
iptables -A INPUT -p tcp --sport 21 -s $UPDATESERVER -j ACCEPT

#defualt policy
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP

#save firewall
sudo iptables-save > /etc/iptables/rules.v4

#list firewall rules
iptables -L -v > /home/alex/configuredstate.log
```

The screenshots above are the Linux script.

Initial State Logs

In this section, I will show the initial list of firewall rules. These firewall rules are saved as ‘initialstate.log’

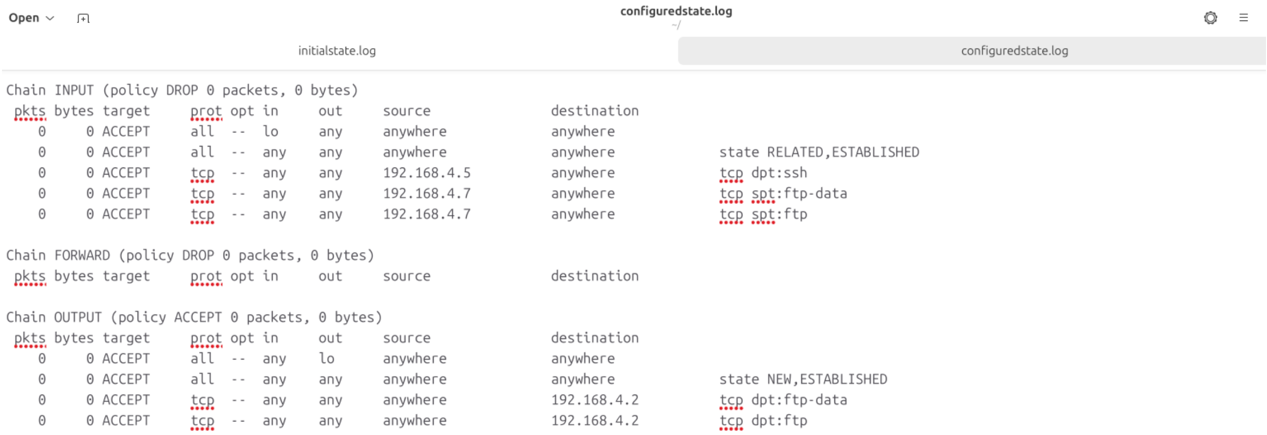


```
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
```

The screenshot above is the initial list of firewalls rules.

Configured State Logs

In this section, I will show the current list of firewall rules. These firewall rules are saved as ‘configuredstate.log’



```
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  lo     any     anywhere             anywhere
    0     0 ACCEPT     all  --  any    any     anywhere             anywhere             state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  any    any     192.168.4.5          anywhere             tcp dpt:ssh
    0     0 ACCEPT     tcp  --  any    any     192.168.4.7          anywhere             tcp spt:ftp-data
    0     0 ACCEPT     tcp  --  any    any     192.168.4.7          anywhere             tcp spt:ftp

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  any    lo      anywhere             anywhere
    0     0 ACCEPT     all  --  any    any     anywhere             anywhere             state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  any    any     anywhere             192.168.4.2          tcp dpt:ftp-data
    0     0 ACCEPT     tcp  --  any    any     anywhere             192.168.4.2          tcp dpt:ftp
```

The screenshot above is the current list of firewall rules.