Assignment 3

Yoshi Ryuzaki, Sukh Atwal

Script

This is a Python2 script where you can configure the number of attempts before blocking, how long you want to block the IP for and the log file directory. You can input these variables as soon as you run the script in the terminal itself where it’s self-explanatory with the raw input.

The script is as follows (I’ve also attached the script file in the zip):

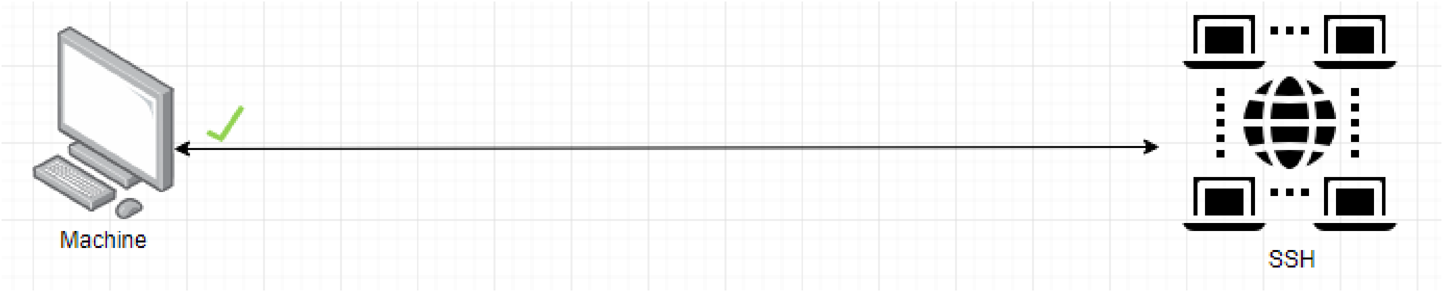
```
import time
import subprocess
from threading import Timer

###################################################################################
################################# USER INPUTS #####################################
###################################################################################

#Number of Attempts Allowed
NumberofAtt=int(raw_input("Please enter the number of attempts allowed before blocking: "))

#Blocking Time
BlockingTime=int(raw_input("How long do you want to block the IP for? Enter in seconds: "))

#Target log file
targetfile=raw_input("Please enter the log file directory: ")

###################################################################################
################################ SCRIPT ###########################################
###################################################################################

#Tracks the log file, equivalent of tail -F
def follow(thefile):
    thefile.seek(0,2)
    while True:
        line = thefile.readline()
        if not line:
            time.sleep(0.1)
            continue
        yield line

#Split each line to a list, getting the IP address from the list
def getip(line):
    elementslist= []
    elements = line.split()
    for element in elements:
        elementslist.append(element)
    #print elementslist
    return elementslist[10]
    #print elementslist[10]


#Track the log
#f = open("/var/log/secure")
f = open(str(targetfile))
lines = follow(f)

#Create dictionary for counting each IP
ipcount = {}
```

```
#Counts each attempt by the IP
for i in lines:
    if (i.find('Failed password')!=-1):
        print i
        ipaddr=getip(i)
        if ipaddr in ipcount:
            ipcount[ipaddr]+= 1
        else:
            ipcount[ipaddr] = 1
        print "This IP has reached "+str(ipcount[ipaddr])+" Attempts"

        #If attempts exceeds the amount entered at the start, drop the IP for the specified amount
of time
        if ipcount[ipaddr] >= NumberofAtt:
            print "More than "+str(NumberofAtt)+" attempts, IP is blocked"
            ipcount[ipaddr] = 0;
            subprocess.call('iptables -A INPUT -s '+ipaddr+' -j DROP',shell=True)
            def release_ip():
                subprocess.call('iptables -D INPUT -s '+ipaddr+' -j DROP',shell=True)

            t= Timer(BlockingTime,release_ip)
            t.start()
    #Clear the counter if user correctly enters the password
    elif (i.find('Accepted password') !=-1):
        ipaddr=getip(i)
        ipcount[ipaddr] = 0
    else:
        continue
```

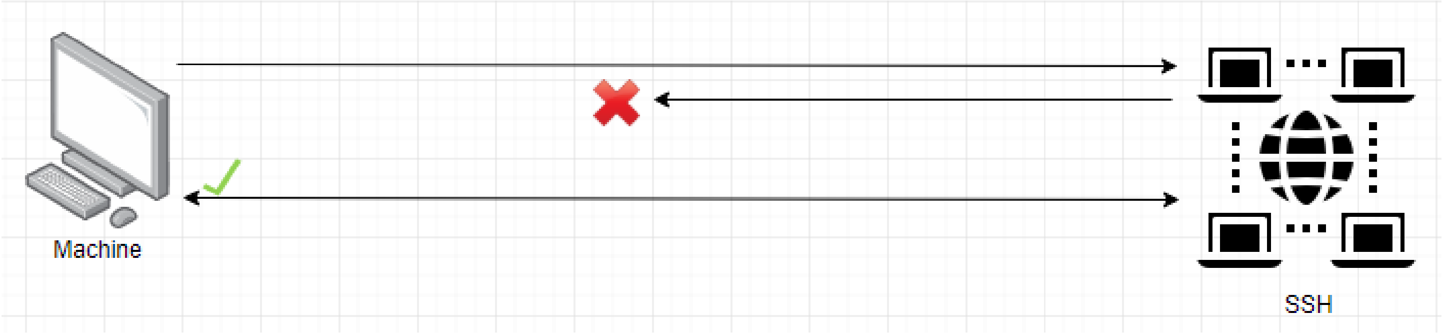
Diagram

For the purposes of this diagram, the maximum number of attempts will be set to 2.

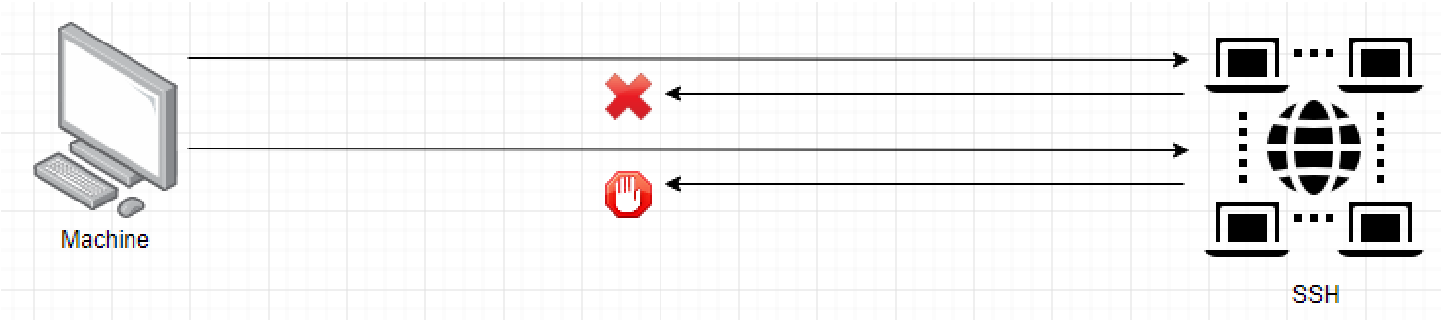
Successful at first attempt:



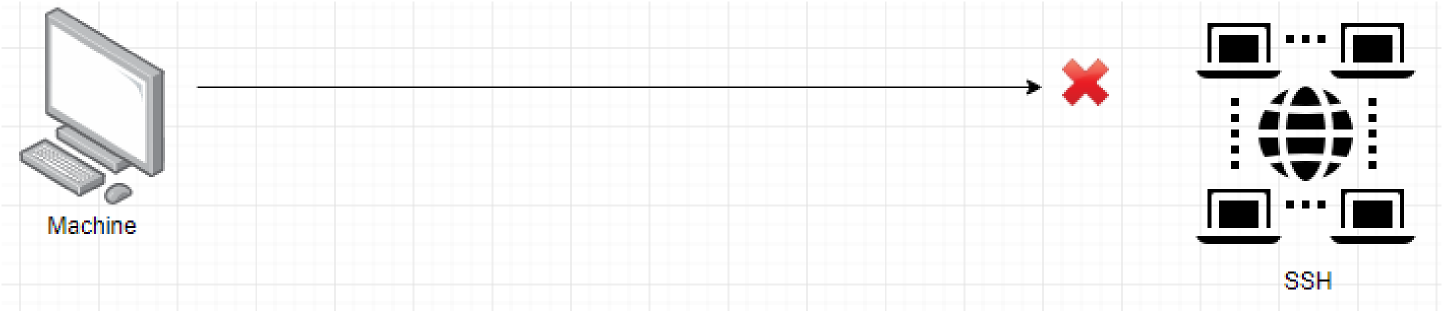
Successful at second attempt:



Failed at second attempt:



Trying to connect before blocked IP time runs out after failing at second attempt:

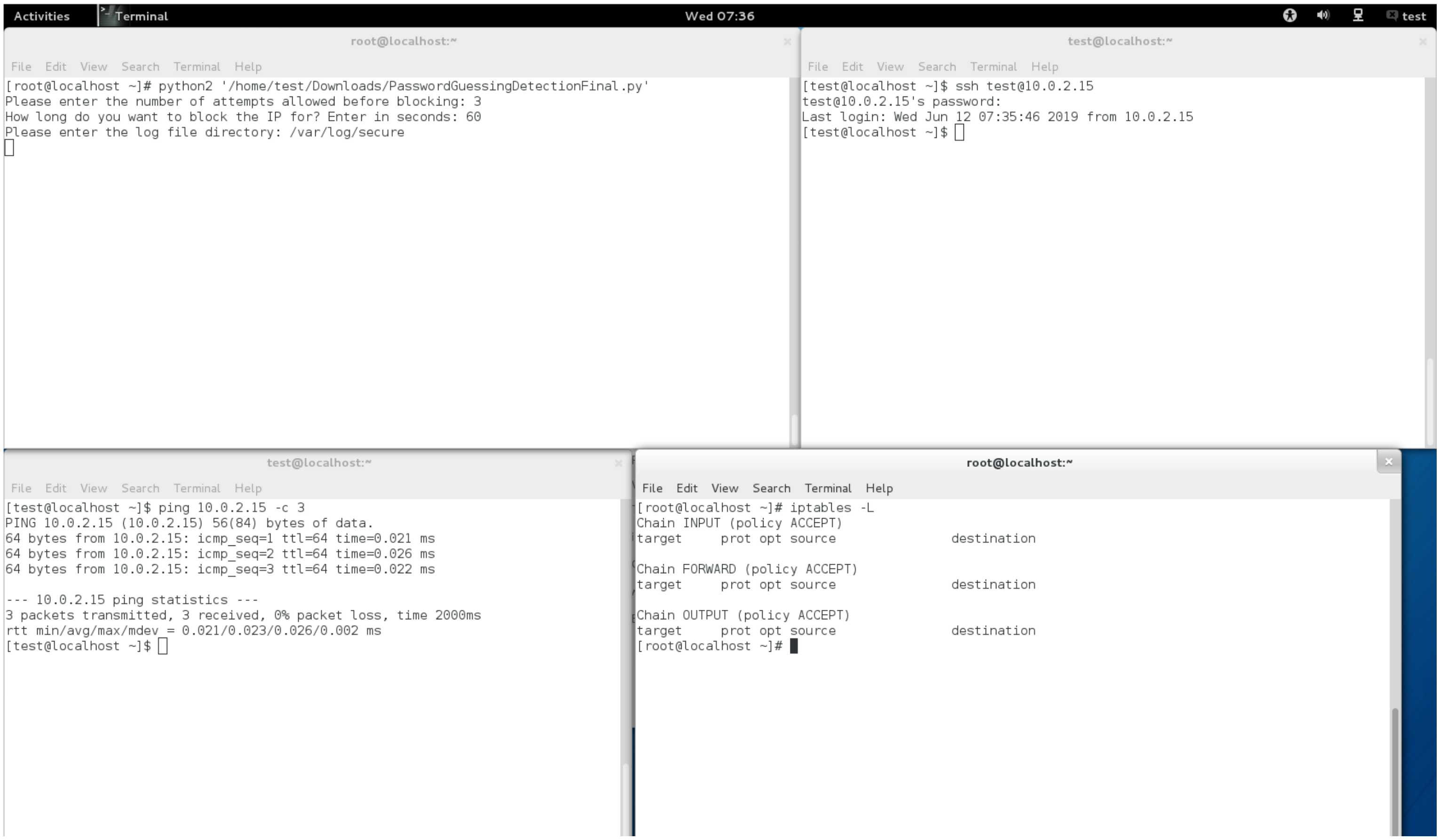


Testing

During this test I set the number of attempts to 3, block time to 60 seconds and log location to /var/log/secure. All of the testing was done on the same machine using Fedora 18 in VirtualBox with IP 10.0.2.15.

Rule #	Test Description	Tools Used	Expected Result	Pass/Fail
1	Correctly typed in the password the first time	Ssh, ping	No output should appear in the script terminal, able to ssh successfully with ping working	Pass
2	Didn't input password correctly the first time	Ssh, ping	Script terminal should output that 1 attempt was made but able to ssh and ping successfully	Pass
3	Didn't input password correctly the second time	Ssh, ping	Script terminal should output that 2 attempts were made but still able to ssh and ping successfully	Pass
4	Didn't input password correctly the third time	Ssh, ping	Script terminal should output that 3 attempts were made and block the IP for the amount of time specified, should not be able to ssh again or ping until the duration is over	Pass
5	Checking if the duration of the blocked time is correct	Ssh, ping	Should be able to ssh and ping 60 seconds after the IP was blocked by the script	Pass

Rule #1


Activities
Terminal
Wed 07:36
test
root@localhost:~
File Edit View Search Terminal Help
test@localhost:~
File Edit View Search Terminal Help
test@localhost:~
File Edit View Search Terminal Help
root@localhost:~
File Edit View Search Terminal Help

```
[root@localhost ~]# python2 '/home/test/Downloads/PasswordGuessingDetectionFinal.py'
Please enter the number of attempts allowed before blocking: 3
How long do you want to block the IP for? Enter in seconds: 60
Please enter the log file directory: /var/log/secure
```

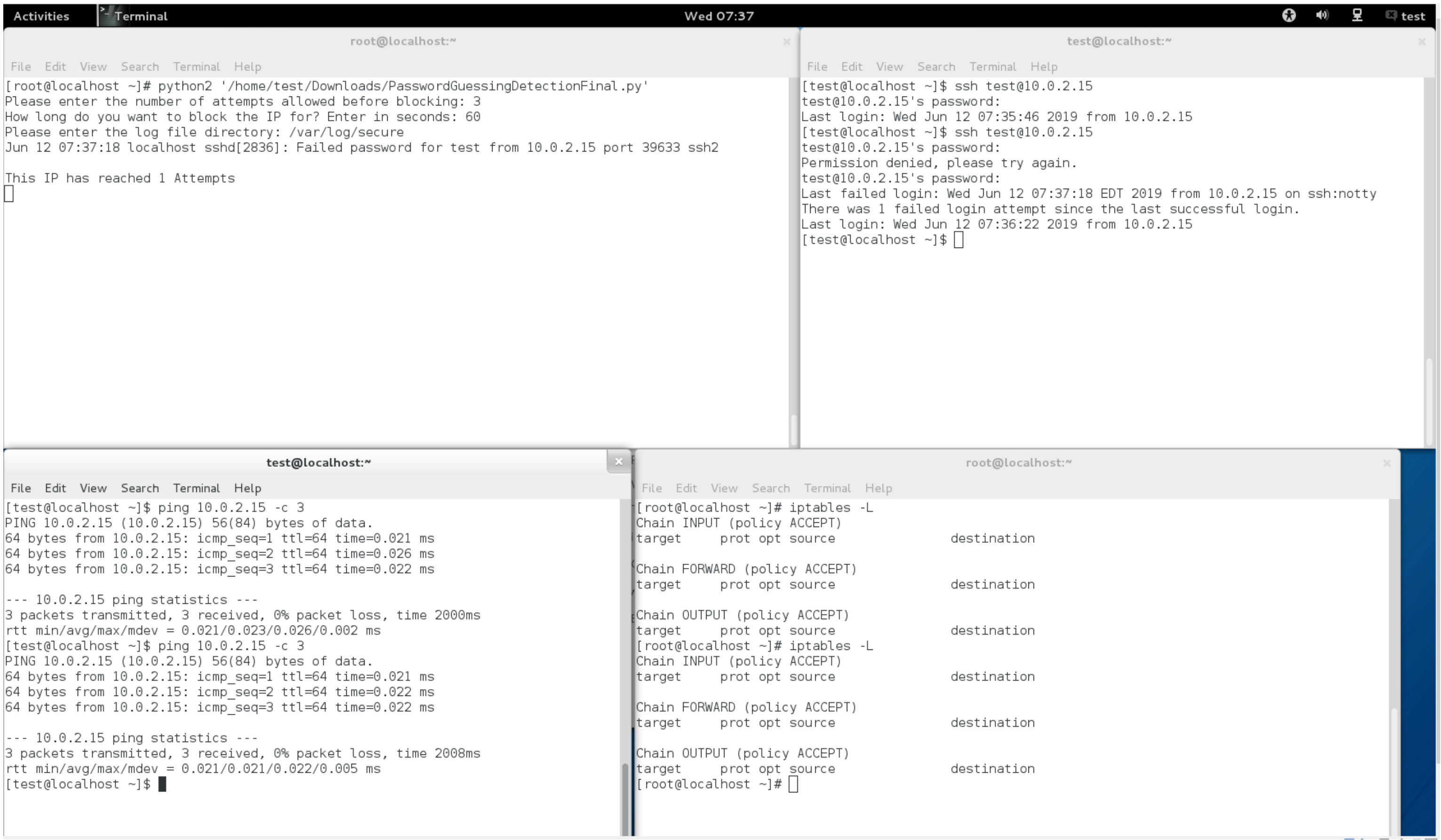
```
[test@localhost ~]$ ssh test@10.0.2.15
test@10.0.2.15's password:
Last login: Wed Jun 12 07:35:46 2019 from 10.0.2.15
[test@localhost ~]$
```

```
[test@localhost ~]$ ping 10.0.2.15 -c 3
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.021 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.026 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.022 ms

--- 10.0.2.15 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.021/0.023/0.026/0.002 ms
[test@localhost ~]$
```

```
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost ~]#
```

On the top left you can see the script running with no output as the password was successfully inputted the first time (As seen on the terminal beside it). We were able to ping successfully, and no changes were made in the iptables.

Rule #2


Activities
Terminal
Wed 07:37
test
root@localhost:~
File Edit View Search Terminal Help
test@localhost:~
File Edit View Search Terminal Help
test@localhost:~
File Edit View Search Terminal Help
root@localhost:~
File Edit View Search Terminal Help

```
[root@localhost ~]# python2 '/home/test/Downloads/PasswordGuessingDetectionFinal.py'
Please enter the number of attempts allowed before blocking: 3
How long do you want to block the IP for? Enter in seconds: 60
Please enter the log file directory: /var/log/secure
Jun 12 07:37:18 localhost sshd[2836]: Failed password for test from 10.0.2.15 port 39633 ssh2

This IP has reached 1 Attempts
```

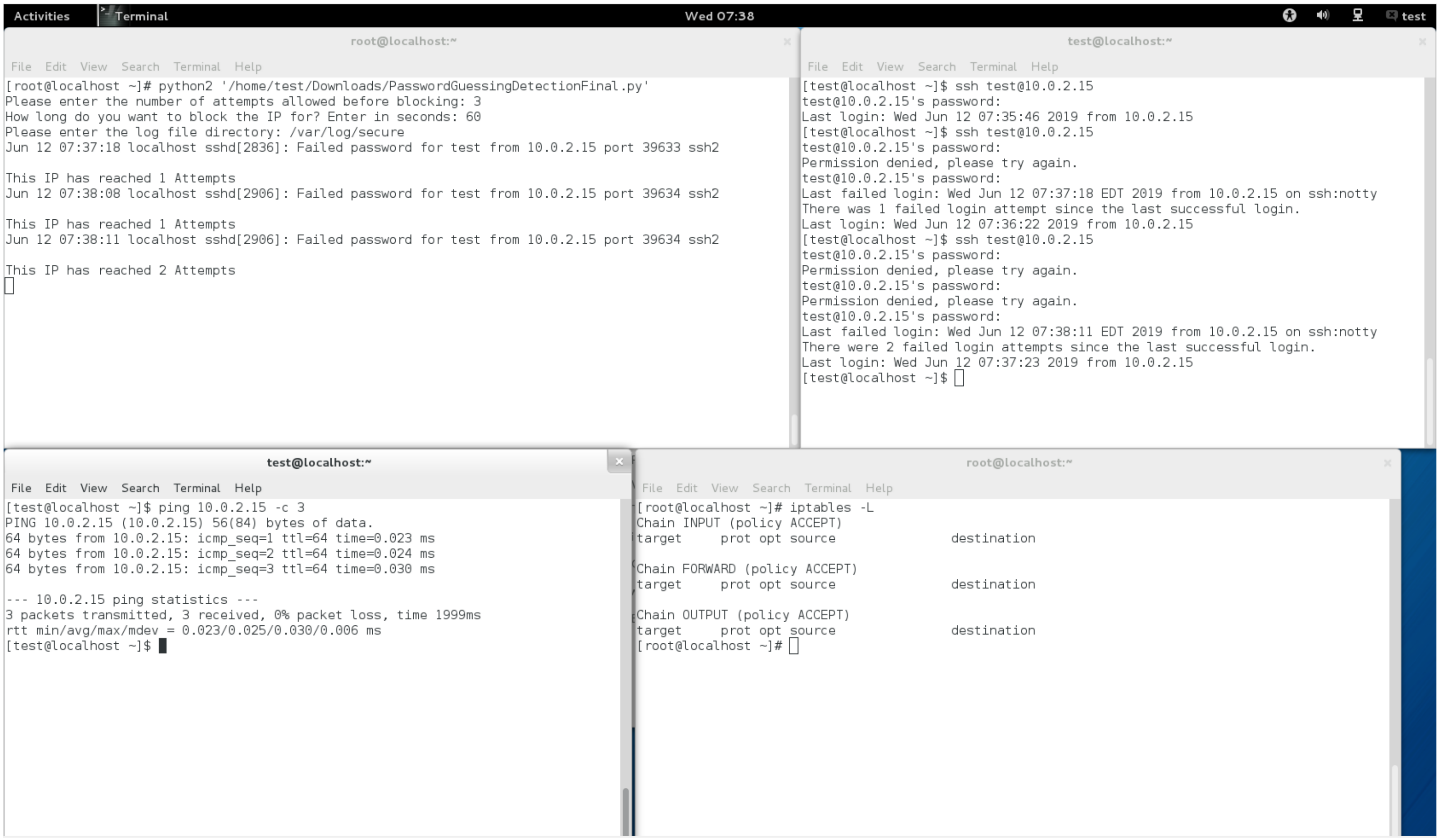
```
[test@localhost ~]$ ssh test@10.0.2.15
test@10.0.2.15's password:
Last login: Wed Jun 12 07:35:46 2019 from 10.0.2.15
[test@localhost ~]$ ssh test@10.0.2.15
test@10.0.2.15's password:
Permission denied, please try again.
test@10.0.2.15's password:
Last failed login: Wed Jun 12 07:37:18 EDT 2019 from 10.0.2.15 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Wed Jun 12 07:36:22 2019 from 10.0.2.15
[test@localhost ~]$
```

```
[test@localhost ~]$ ping 10.0.2.15 -c 3
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.021 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.026 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.022 ms

--- 10.0.2.15 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.021/0.023/0.026/0.002 ms
[test@localhost ~]$ ping 10.0.2.15 -c 3
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.021 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.022 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.022 ms

--- 10.0.2.15 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 0.021/0.021/0.022/0.005 ms
[test@localhost ~]$
```

```
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost ~]#
```

Similar to the previous screen however this time it showcases there was 1 failed attempt alongside the IP and port it came from. The password was successful after, so we were able to ping and iptables showed no changes again.

Rule #3


Activities
Terminal
Wed 07:38
test
root@localhost:~
File Edit View Search Terminal Help
test@localhost:~
File Edit View Search Terminal Help
test@localhost:~
File Edit View Search Terminal Help
root@localhost:~
File Edit View Search Terminal Help

```
[root@localhost ~]# python2 '/home/test/Downloads/PasswordGuessingDetectionFinal.py'
Please enter the number of attempts allowed before blocking: 3
How long do you want to block the IP for? Enter in seconds: 60
Please enter the log file directory: /var/log/secure
Jun 12 07:37:18 localhost sshd[2836]: Failed password for test from 10.0.2.15 port 39633 ssh2

This IP has reached 1 Attempts
Jun 12 07:38:08 localhost sshd[2906]: Failed password for test from 10.0.2.15 port 39634 ssh2

This IP has reached 1 Attempts
Jun 12 07:38:11 localhost sshd[2906]: Failed password for test from 10.0.2.15 port 39634 ssh2

This IP has reached 2 Attempts
```

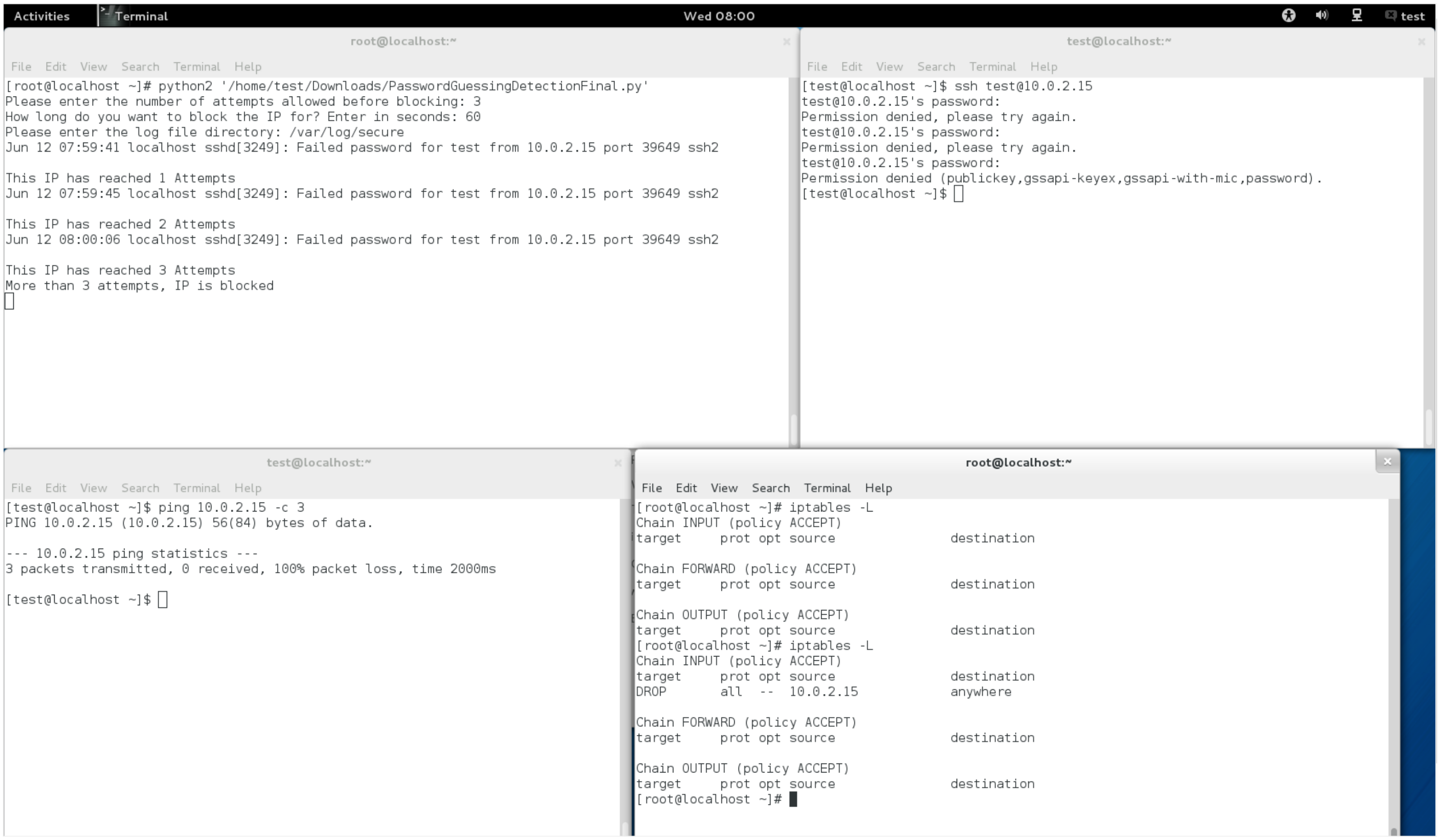
```
[test@localhost ~]$ ssh test@10.0.2.15
test@10.0.2.15's password:
Last login: Wed Jun 12 07:35:46 2019 from 10.0.2.15
[test@localhost ~]$ ssh test@10.0.2.15
test@10.0.2.15's password:
Permission denied, please try again.
test@10.0.2.15's password:
Last failed login: Wed Jun 12 07:37:18 EDT 2019 from 10.0.2.15 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Wed Jun 12 07:36:22 2019 from 10.0.2.15
[test@localhost ~]$ ssh test@10.0.2.15
test@10.0.2.15's password:
Permission denied, please try again.
test@10.0.2.15's password:
Permission denied, please try again.
test@10.0.2.15's password:
Last failed login: Wed Jun 12 07:38:11 EDT 2019 from 10.0.2.15 on ssh:notty
There were 2 failed login attempts since the last successful login.
Last login: Wed Jun 12 07:37:23 2019 from 10.0.2.15
[test@localhost ~]$
```

```
[test@localhost ~]$ ping 10.0.2.15 -c 3
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.023 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.024 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.030 ms

--- 10.0.2.15 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.023/0.025/0.030/0.006 ms
[test@localhost ~]$
```

```
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost ~]#
```

Same as before with the only difference being there was 2 failed attempts.

Rule #4


Activities
Terminal
Wed 08:00
test
root@localhost:~
File Edit View Search Terminal Help
test@localhost:~
File Edit View Search Terminal Help
test@localhost:~
File Edit View Search Terminal Help
root@localhost:~
File Edit View Search Terminal Help

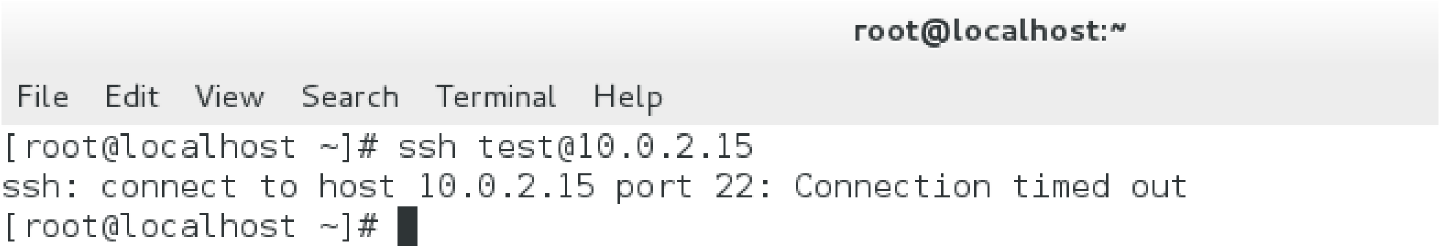
```
[root@localhost ~]# python2 '/home/test/Downloads/PasswordGuessingDetectionFinal.py'
Please enter the number of attempts allowed before blocking: 3
How long do you want to block the IP for? Enter in seconds: 60
Please enter the log file directory: /var/log/secure
Jun 12 07:59:41 localhost sshd[3249]: Failed password for test from 10.0.2.15 port 39649 ssh2

This IP has reached 1 Attempts
Jun 12 07:59:45 localhost sshd[3249]: Failed password for test from 10.0.2.15 port 39649 ssh2

This IP has reached 2 Attempts
Jun 12 08:00:06 localhost sshd[3249]: Failed password for test from 10.0.2.15 port 39649 ssh2

This IP has reached 3 Attempts
More than 3 attempts, IP is blocked
```

```
[test@localhost ~]$ ssh test@10.0.2.15
test@10.0.2.15's password:
Permission denied, please try again.
test@10.0.2.15's password:
Permission denied, please try again.
test@10.0.2.15's password:
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[test@localhost ~]$
```

```
[test@localhost ~]$ ping 10.0.2.15 -c 3
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.

--- 10.0.2.15 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2000ms

[test@localhost ~]$
```

```
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  10.0.2.15            anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost ~]#
```

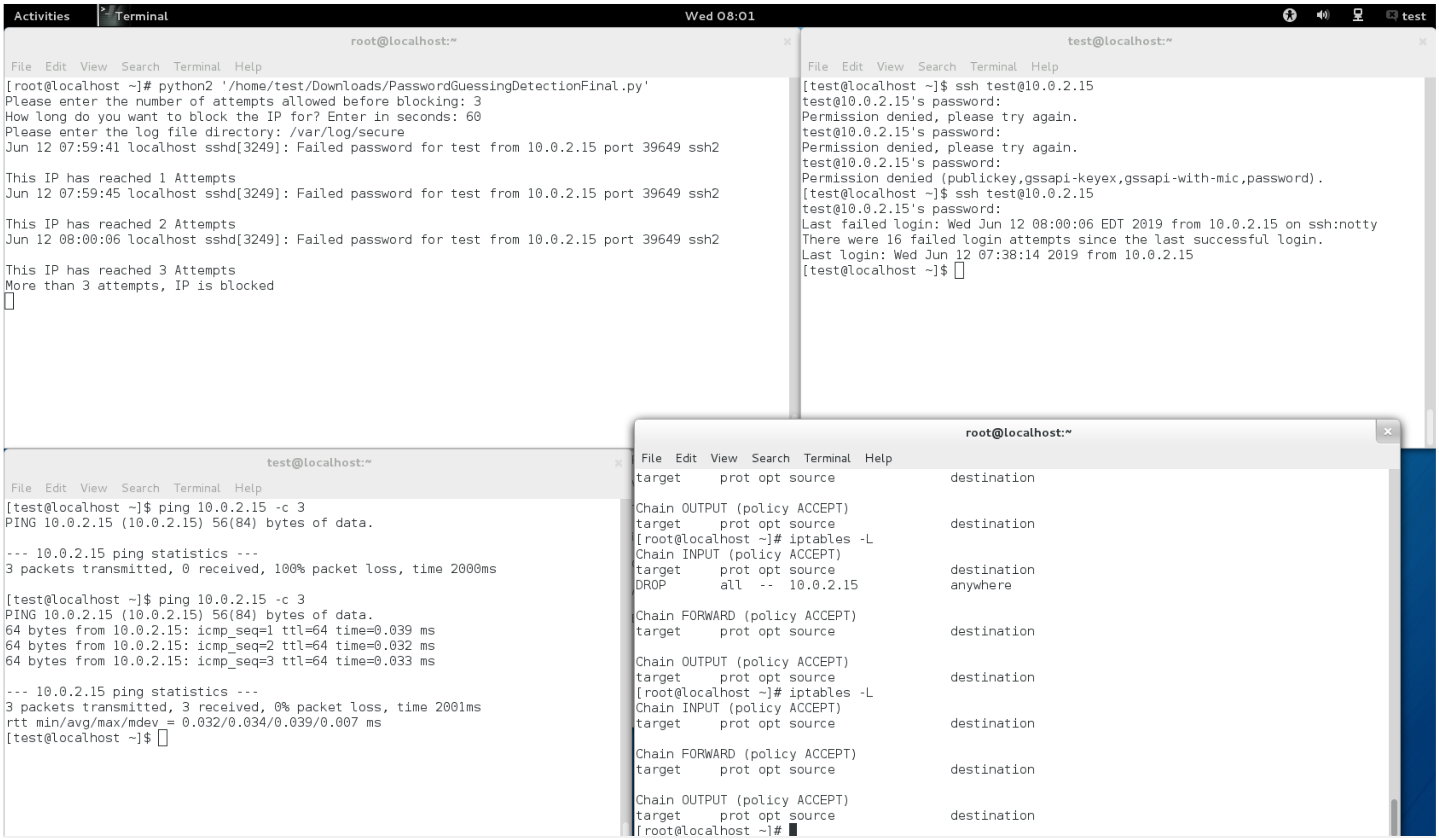
Here we reached the maximum attempts that we set which was 3. It blocked the IP and set it to DROP in the iptables. We were also unable to ping successfully anymore.



```
[root@localhost ~]# ssh test@10.0.2.15
ssh: connect to host 10.0.2.15 port 22: Connection timed out
[root@localhost ~]#
```

Attempted to try to ssh again however the connection timed out as the IP was still blocked.

Rule #5


Activities
Terminal
Wed 08:01
test
root@localhost:~
File Edit View Search Terminal Help
test@localhost:~
File Edit View Search Terminal Help
test@localhost:~
File Edit View Search Terminal Help
root@localhost:~
File Edit View Search Terminal Help

```
[root@localhost ~]# python2 '/home/test/Downloads/PasswordGuessingDetectionFinal.py'
Please enter the number of attempts allowed before blocking: 3
How long do you want to block the IP for? Enter in seconds: 60
Please enter the log file directory: /var/log/secure
Jun 12 07:59:41 localhost sshd[3249]: Failed password for test from 10.0.2.15 port 39649 ssh2

This IP has reached 1 Attempts
Jun 12 07:59:45 localhost sshd[3249]: Failed password for test from 10.0.2.15 port 39649 ssh2

This IP has reached 2 Attempts
Jun 12 08:00:06 localhost sshd[3249]: Failed password for test from 10.0.2.15 port 39649 ssh2

This IP has reached 3 Attempts
More than 3 attempts, IP is blocked
```

```
[test@localhost ~]$ ssh test@10.0.2.15
test@10.0.2.15's password:
Permission denied, please try again.
test@10.0.2.15's password:
Permission denied, please try again.
test@10.0.2.15's password:
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[test@localhost ~]$ ssh test@10.0.2.15
test@10.0.2.15's password:
Last failed login: Wed Jun 12 08:00:06 EDT 2019 from 10.0.2.15 on ssh:notty
There were 16 failed login attempts since the last successful login.
Last login: Wed Jun 12 07:38:14 2019 from 10.0.2.15
[test@localhost ~]$
```

```
[test@localhost ~]$ ping 10.0.2.15 -c 3
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.

--- 10.0.2.15 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2000ms

[test@localhost ~]$ ping 10.0.2.15 -c 3
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.039 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.032 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.033 ms

--- 10.0.2.15 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.032/0.034/0.039/0.007 ms
[test@localhost ~]$
```

```
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  10.0.2.15            anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost ~]#
```

After 60 seconds passed which was the duration we set, the iptables rule to drop that IP was removed and we were able to successfully ping and ssh again.