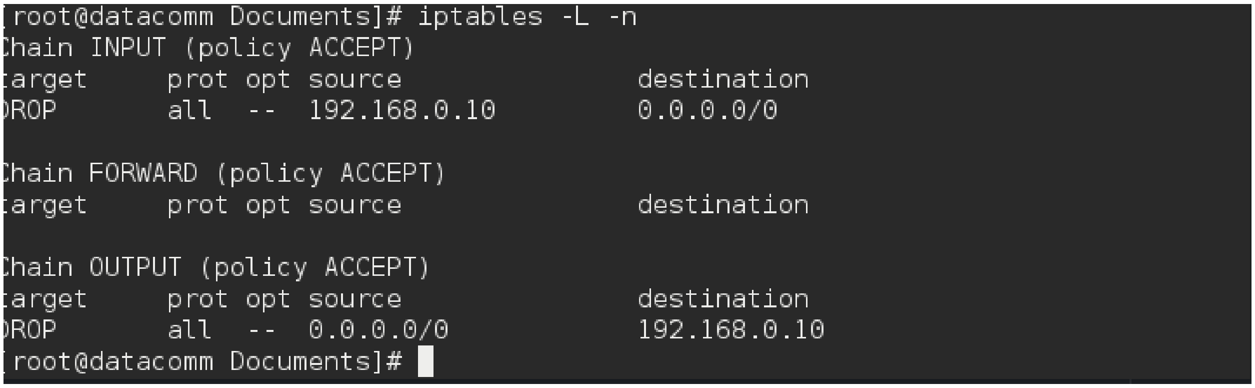
Testing Document

Test Cases

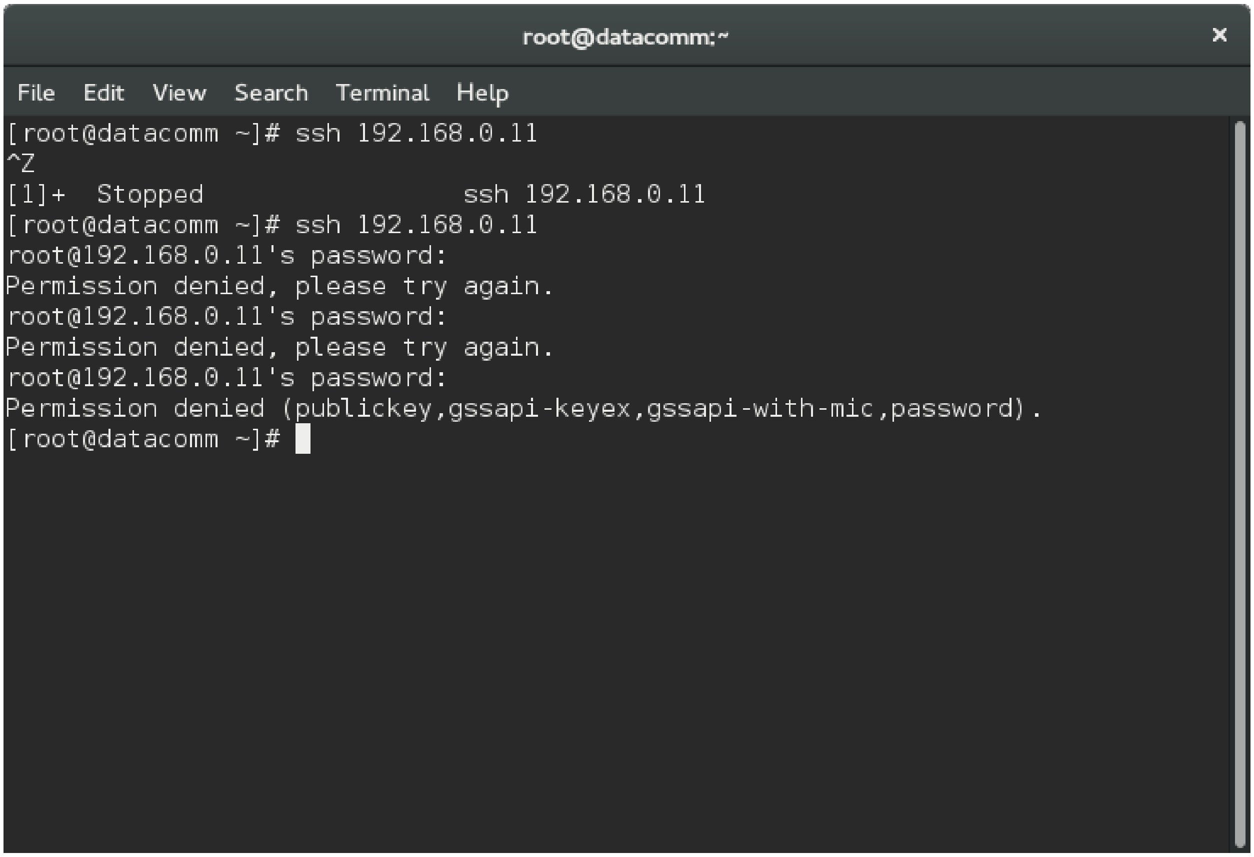
Rule #	Test Description	Tool Used	Expected Result	Pass/Fail
1	Block at attempts above User specified attempts	SSH Server, crontab	The script should add an entry to the iptables rules to DROP the traffic	Pass
2	No Block at number of attempts less than user specified attempts	SSH Server, crontab	The number of attempts made are less than the number of allowed attempts therefore the ip is not blocked	Pass
3	Block the IP for a certain Time limit	SSH server, crontab	The IP should be removed from the iptables entry after a certain time period	FAIL

Test Case1:

- The following test was conducted by adding the IP to the iptables using netfilter.
- There were 4 incorrect password attempts
- The user specified allowed attempts were 3
- This Ip was blocked



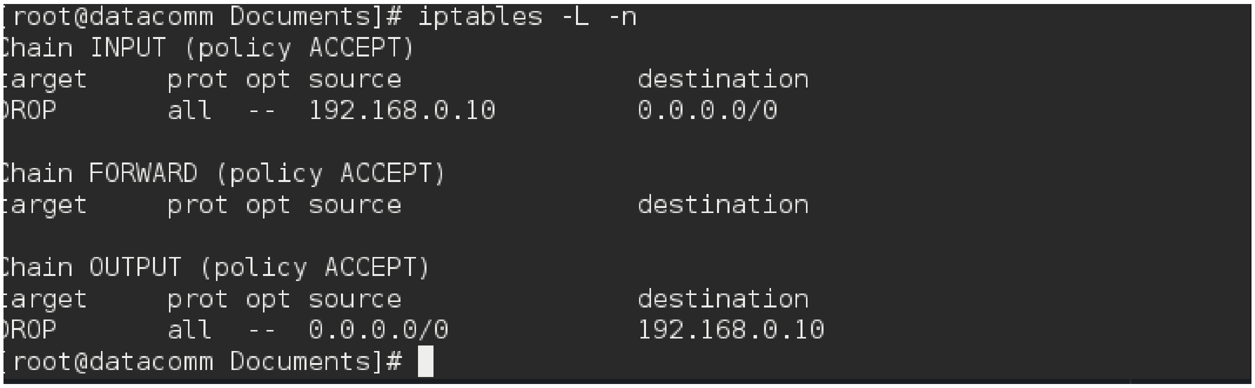
```
[root@datacomm Documents]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.0.10         0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  0.0.0.0/0            192.168.0.10
[root@datacomm Documents]# 
```



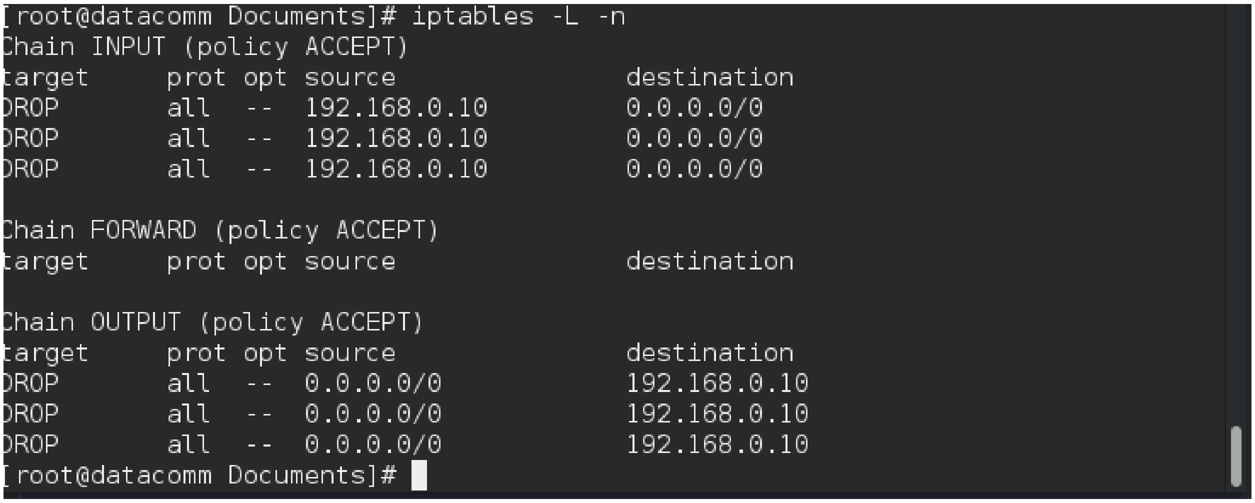
```
[root@datacomm ~]# ssh 192.168.0.11
^Z
[1]+  Stopped                 ssh 192.168.0.11
[root@datacomm ~]# ssh 192.168.0.11
root@192.168.0.11's password:
Permission denied, please try again.
root@192.168.0.11's password:
Permission denied, please try again.
root@192.168.0.11's password:
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@datacomm ~]# 
```

Test Case2:

- The allowed number of attempts were 3
- User tried 2 times with wrong password
- The Ip was not blocked



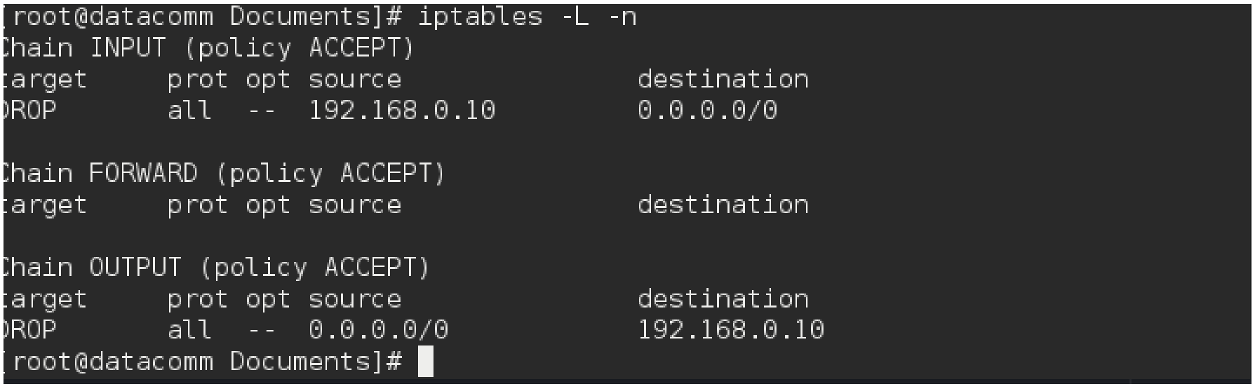
```
[root@datacomm Documents]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.0.10         0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  0.0.0.0/0            192.168.0.10
[root@datacomm Documents]#
```



```
[root@datacomm Documents]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.0.10         0.0.0.0/0
DROP       all  --  192.168.0.10         0.0.0.0/0
DROP       all  --  192.168.0.10         0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  0.0.0.0/0            192.168.0.10
DROP       all  --  0.0.0.0/0            192.168.0.10
DROP       all  --  0.0.0.0/0            192.168.0.10
[root@datacomm Documents]#
```

Test Case 3:

- User specified time limit to be 3 minutes
- The IP is to be removed from the iptables
- This was not successful as the entry was still in the iptables



```
[root@datacomm Documents]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.0.10         0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  0.0.0.0/0            192.168.0.10
[root@datacomm Documents]# 
```