**Computer Systems Technology**

British Columbia Institute of Technology

COMP 8006 - Assignment3- Testing

Albert Huang &

Aiyan Ma

Feb 20, 2018

# Table of Contents

[Table of Contents 2](#_Toc28122)

[1. Monitor Testing 3](#_Toc19908)

[1.1 Test Outline 3](#_Toc2792)

[1.2 Test Case Descriptions 6](#_Toc14978)

[1.2.1 Test 1 6](#_Toc15765)

[1.2.3 Test 3 6](#_Toc27113)

[1.2.4 Test 4 6](#_Toc17078)

[Test5 7](#_Toc25507)

[Test 9 8](#_Toc28881)

[Test 10 8](#_Toc25497)

# Monitor Testing

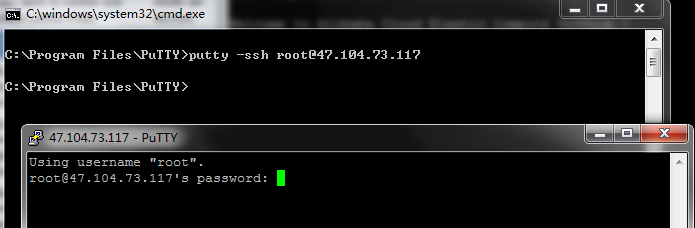
## 1.1 Test Outline

| Rule # | Test Description | Tool Used | Expected Results | Pass/Fail |
| --- | --- | --- | --- | --- |
| 1 | Successfully use command line interface start monitor | Bash/vim | Monitor start from command line interface, and record a password attempt in blacklist | Pass. Detailed results are attached. |
| 2 | Successfully use regular expression tester to test user defined pattern | Bash | Try regular expression tester many times to confirm user defined pattern works | Pass. Detailed results are attached. |
| SSH Service | | | | |
| 3 | Successfully login SSH server | SSH client | The application won’t match anything  (command: #ssh server\_ip) | Pass. Detailed results are attached. |
| 4 | Fail to input the correct password and matched by default method (awk) | SSH client | The application would match the record from log file, and add or update the record to the blacklist  (command: #ssh server\_ip) | Pass. Detailed results are attached. |
| 5 | Fail to input the correct password and matched by regular expression | SSH client | The application would match the record from log file, and add or update the record to the blacklist  (command: #ssh server\_ip) | Pass. Detailed results are attached. |
| 6 | More than one visitor fail to input the correct password | SSH client | The application would match the record from log file, and add the new record into the blacklist  (command: #ssh server\_ip) | Pass. Detailed results are attached. |
| 7 | One visitor try many times and then get blocked through iptables | SSH client & iptables | The application would match the record from log file, and delete the record from the blacklist  The iptables add a rule of blocking visitor.  (command: #ssh server\_ip)  (command: #iptables -L) | Pass. Detailed results are attached. |
| 8 | More than one visitors try many times and then get blocked through iptables | SSH client & iptables | The application would match the record from log file, and delete the record from the blacklist  The iptables add a rules of blocking visitors.  (command: #ssh server\_ip)  (command: #iptables -L) | Pass. Detailed results are attached. |
| 9 | Crontab task activate the application | crontab | The application would activate through crontab  (\* \* \* \* \* /app path/monitor.sh timelimit $target\_ip $port) | Pass. Detailed results are attached. |
| 10 | After blocking period the visitor can access SSH service again | SSH client & iptables | After the blocking period, the blocking rule will be deleted, the visitor could access the ssh server again  (command: #iptables -L)  (command: #ssh server\_ip) | Pass. Detailed results are attached. |
| FTP Service | | | | |
| 11 | Successfully login FTP server | FTP client | The application won’t match anything  (command: #ftp server\_ip) | Pass. Detailed results are attached. |
| 12 | Fail to input the correct password and matched by default method (awk) | FTP client | The application would match the record from log file, and add or update the record to the blacklist  (command: #ftp server\_ip) | Pass. Detailed results are attached. |
| 13 | Fail to input the correct password and matched by regular expression | FTP client | The application would match the record from log file, and add or update the record to the blacklist  (command: #ftp server\_ip) | Pass. Detailed results are attached. |
| 14 | More than one visitor fail to input the correct password | FTP client | The application would match the record from log file, and add the new record into the blacklist  (command: #ftp server\_ip) | Pass. Detailed results are attached. |
| 15 | One visitor try many times and then get blocked through iptables | FTP client& iptables | The application would match the record from log file, and delete the record from the blacklist  The iptables add a rule of blocking visitor.  (command: #iptables -L) | Pass. Detailed results are attached. |
| 16 | More than one visitors try many times and then get blocked through iptables | FTP client & iptables | The application would match the record from log file, and delete the record from the blacklist  The iptables add a rules of blocking visitors.  (command: #ftp server\_ip)  (command: #iptables -L) | Pass. Detailed results are attached. |
| 17 | Crontab task activate the application | crontab | The application would activate through crontab  (\* \* \* \* \* /app path/monitor.sh timelimit $target\_ip $port) | Pass. Detailed results are attached. |
| 18 | After blocking period the visitor can access FTP service again | FTP client& iptables | After the blocking period, the blocking rule will be deleted, the visitor could access the ssh server again  (command: #iptables -L)  (command: #ftp server\_ip) | Pass. Detailed results are attached. |

## 1.2 Test Case Descriptions

### 1.2.1 Test 1

### 1.2.3 Test 3



### 1.2.4 Test 4

**Fail to get the IP**

The IP is not correctly retrieved, it should be 75.157.65.60

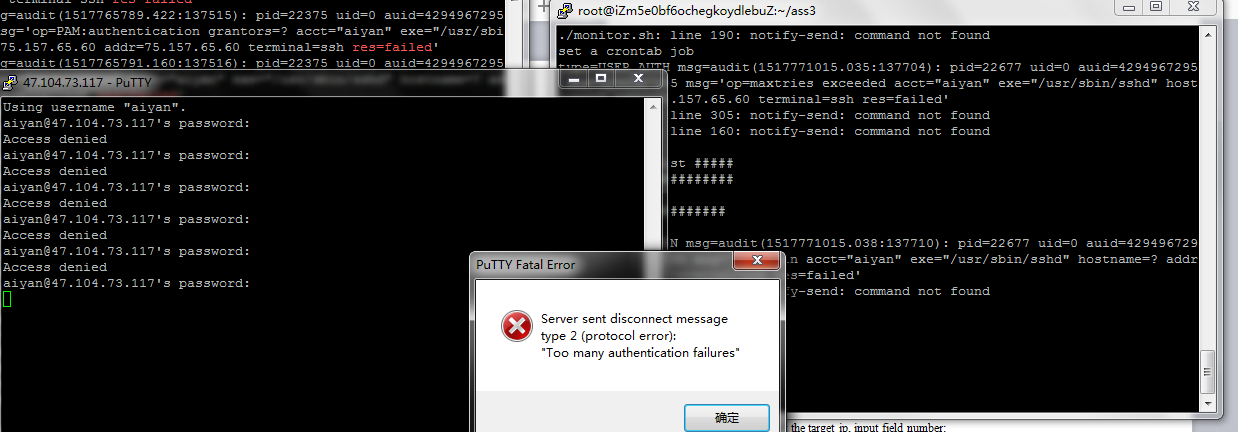
But the iptable rules is:

Chain INPUT (policy ACCEPT)

target prot opt source destination

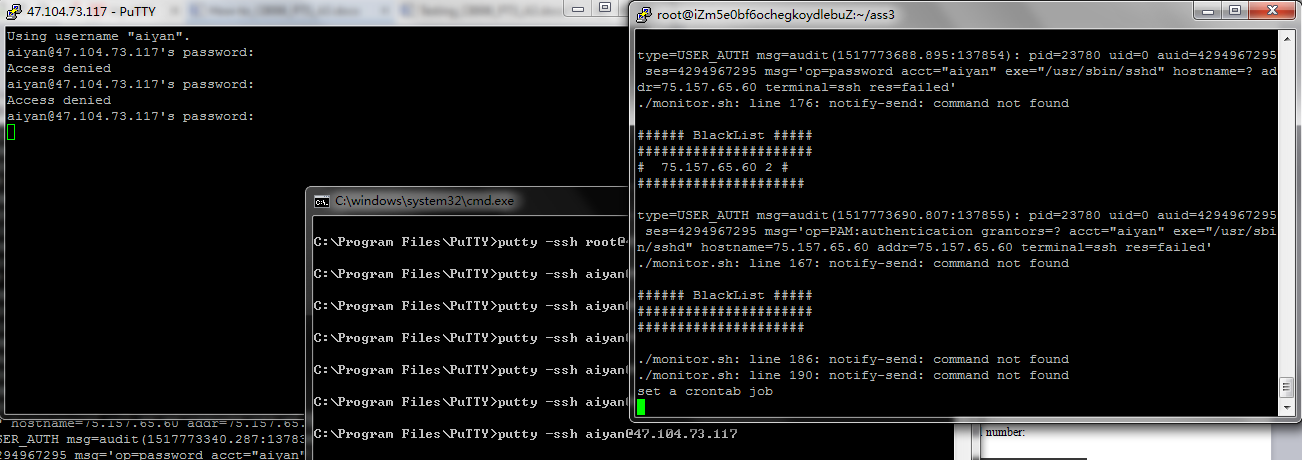
DROP tcp -- 13.0.0.0 anywhere tcp dpt:ssh

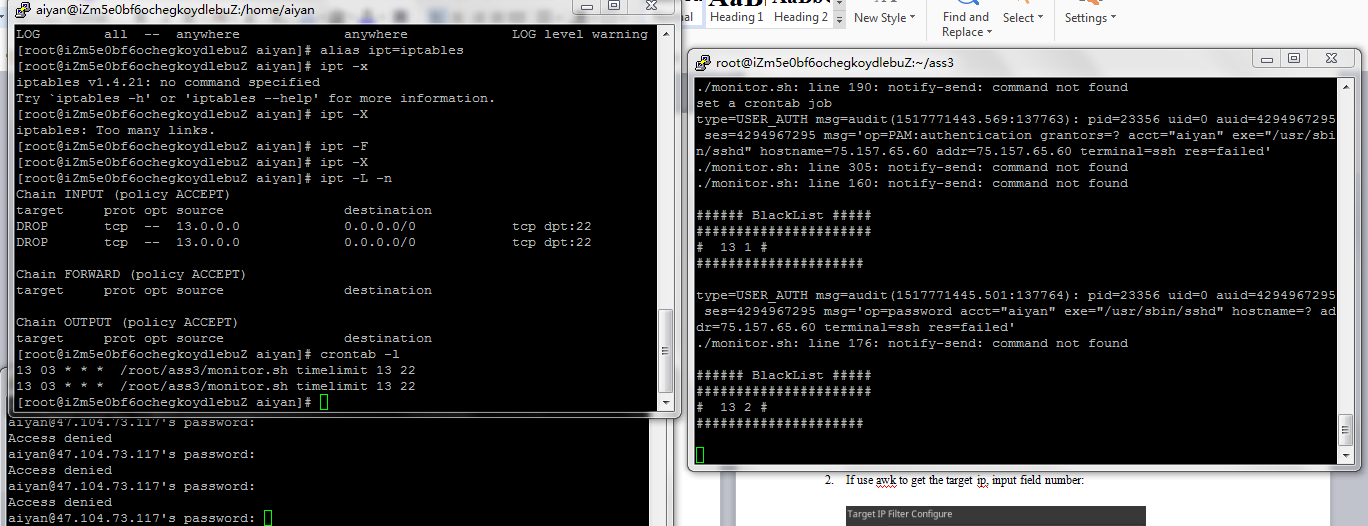
type=USER\_AUTH msg=audit(1517773338.007:137835): pid=23675 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication grantors=? acct="aiyan" exe="/usr/sbin/sshd" hostname=75.157.65.60 addr=75.157.65.60 terminal=ssh res=failed'



### Test5

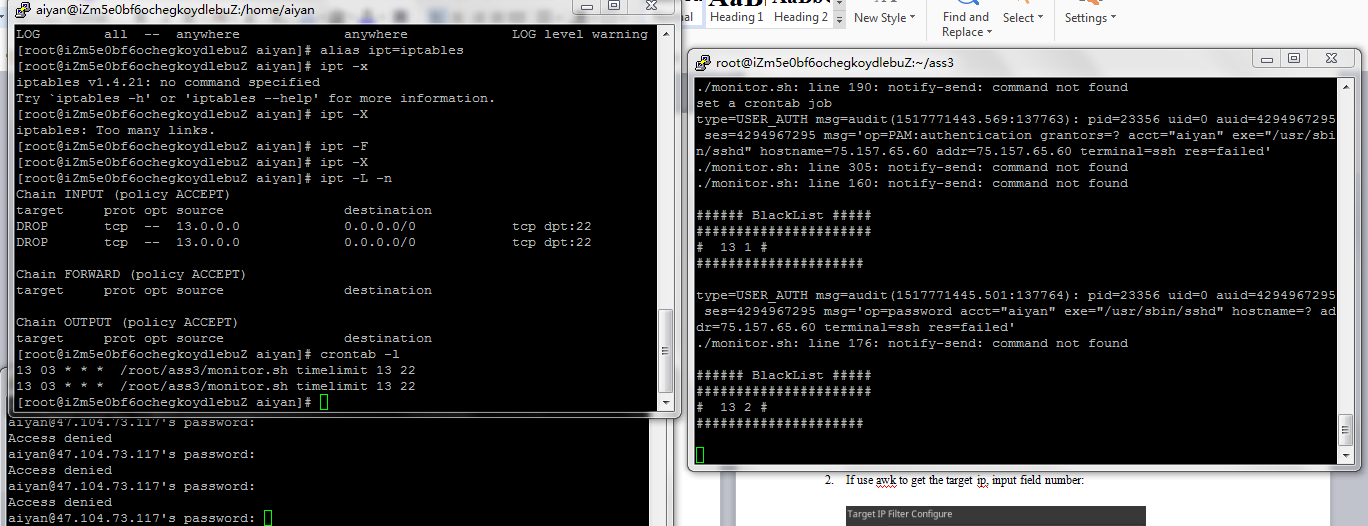
Set the regx=1 to turn on the regx, Lost connection after 3 times wrong password input. PASS





### Test 9

There are crontab jobs when blocking: PASS

s

### Test 10

After 3 minutes, the sshd server is accessible as below. PASS

