COMP 8006 Assignment 3 Testing

Alex Zielinski

03/08/2018

Contents

Testing Explained

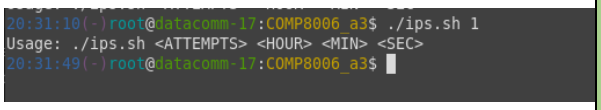
Two machines were used for testing. The machine that was used to run the server with the intrusion detection system has the IP of 192.168.0.17, while the client that is trying to SSH into it has an IP of 192.168.0.18.

Test Cases

Program Usage Tests

Test Case #1	Expected	Screenshot(s)	Result
Steps: 1. Run the client program as follows **./ips.sh** 2. Notice the terminal output	Error will pop up indicate the programs usage.		**PASS**

Incorrect user arguments (1)

Test Case #2	Expected	Screenshot(s)	Result
Steps: 1. Run the client program as follows **./ips.sh 1** 2. Run the client program as follows	Error will pop up indicate the programs usage.		**PASS**

Incorrect user arguments (2)

Test Case #3	Expected	Screenshot(s)	Result
Steps: 1. Run the client program as follows **./ips.sh 1 1** 3. Notice the terminal output	Error will pop up indicate the programs usage.		**PASS**

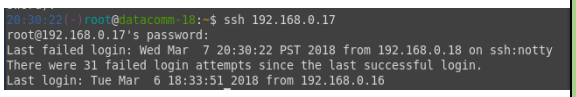
Incorrect user arguments (3)

Test Case #4	Expected	Screenshot(s)	Result
Steps: 1. Run the client program as follows **./ips.sh 1 1 1** 4. Notice the terminal output	Error will pop up indicate the programs usage.		**PASS**

Correct user arguments inputted

Test Case #5	Expected	Screenshot(s)	Result
Steps: 1. Run the client program as follows **./ips.sh 1 1 1 4** 2. Notice the terminal output	Terminal indicates that program has started. Program is running correctly.		**PASS**

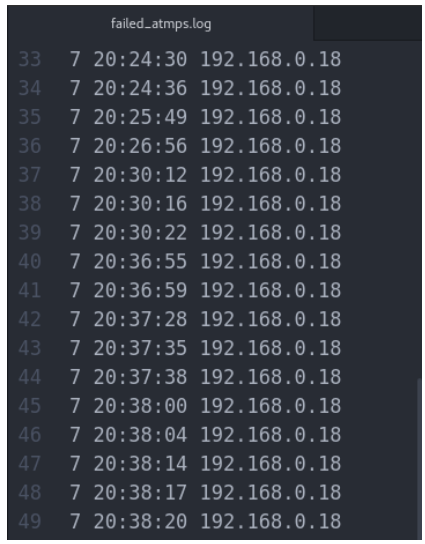
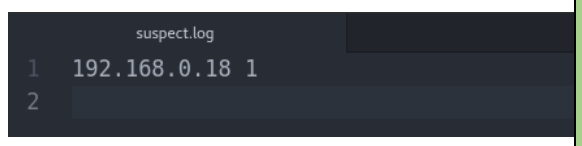
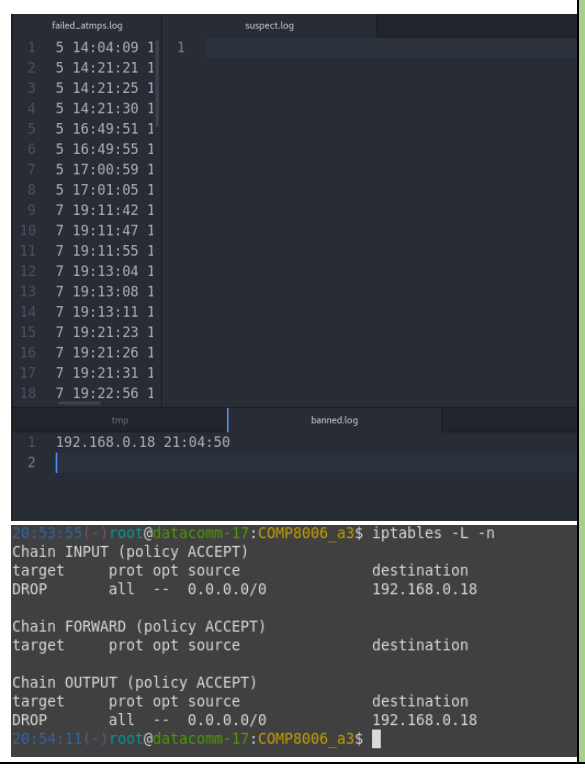
SSH into client with correct password

Test Case #6	Expected	Screenshot(s)	Result
Steps: 1. Run the client program as follows on one computer **./ips.sh 1 1 1 4** 2. Find the IP of the client computer by typing in terminal the following command **./ifconfig** 3. On another computer, run the following command in terminal **ssh *ip*** Note: IP indicates the IP of the client computer found in step 2 4. Type in the correct password. 5. Notice the message displayed on second computer. 6. Check the files to indicate that user is now ssh'd into client.	User can successfully run the program with no errors. The IP of the computer is found, and user can SSH into the client computer after typing in the correct password. Files on client computer are now displayed from user after SSH.		**PASS**

SSH into computer with incorrect password

Test Case #7	Expected	Screenshot(s)	Result
Steps: 1. Run the client program as follows on one computer **./ips.sh 1 1 1 4** 2. Find the IP of the client computer by typing in terminal the following command **./ifconfig** 3. On another computer, run the following command in terminal **ssh *ip*** Note: IP indicates the IP of the client computer found in step 2 4. Type in an ***incorrect*** password 5. Notice the message displayed on second computer.	User can successfully run the program with no errors. The IP of the computer is found, and user is displayed incorrect password message after attempting to SSH into client with wrong password. Suspect log file should have entry of IP.	Client side 20:36:49(-)root@datacomm-18:~$ ssh root@192.168.0.17's password: Permission denied, please try again root@192.168.0.17's password: Permission denied, please try again root@192.168.0.17's password: Log files failed_atmps.log 7 20:24:30 192.168.0.18 7 20:24:36 192.168.0.18 7 20:25:49 192.168.0.18 7 20:26:56 192.168.0.18 7 20:30:12 192.168.0.18 7 20:30:16 192.168.0.18 7 20:30:22 192.168.0.18 7 20:36:55 192.168.0.18 7 20:36:59 192.168.0.18 7 20:37:28 192.168.0.18 7 20:37:35 192.168.0.18 7 20:37:38 192.168.0.18 7 20:38:00 192.168.0.18 7 20:38:04 192.168.0.18 7 20:38:14 192.168.0.18 7 20:38:17 192.168.0.18 7 20:38:20 192.168.0.18 suspect.log 192.168.0.18 14	**PASS**

IP is banned after incorrect attempt limit reached (4 tries)

Test Case #8	Expected	Screenshot(s)	Result
Steps: 1. Run the client program as follows on one computer **./ips.sh 1 1 1 4** 2. Find the IP of the client computer by typing in terminal the following command **./ifconfig** 3. On another computer, run the following command in terminal **ssh *ip*** Note: IP indicates the IP of the client computer found in step 2 4. Type in an ***<u>incorrect</u>*** password **<u>four times</u>** 5. Attempt to login with correct password 6. Notice the message displayed on second computer.	User can successfully run the program with no errors. The IP of the computer is found, and user is displayed incorrect password message after attempting to SSH into client with wrong password. After four attempts, user's IP is banned and cannot login even with correct password. Failed attempt logs show correct IP attempting to connect Check the Suspect file in the COMP8006_a3 folder to ensure IP is banned. Check IP tables to ensure IP is banned. Check Ban file to ensure IP is in ban file.	Log Files  failed_atmps.log 7 20:24:30 192.168.0.18 7 20:24:36 192.168.0.18 7 20:25:49 192.168.0.18 7 20:26:56 192.168.0.18 7 20:30:12 192.168.0.18 7 20:30:16 192.168.0.18 7 20:30:22 192.168.0.18 7 20:36:55 192.168.0.18 7 20:36:59 192.168.0.18 7 20:37:28 192.168.0.18 7 20:37:35 192.168.0.18 7 20:37:38 192.168.0.18 7 20:38:00 192.168.0.18 7 20:38:04 192.168.0.18 7 20:38:14 192.168.0.18 7 20:38:17 192.168.0.18 7 20:38:20 192.168.0.18  suspect.log 192.168.0.18 1  failed_atmps.log 5 14:04:09 1 5 14:21:21 1 5 14:21:25 1 5 14:21:30 1 5 16:49:51 1 5 16:49:55 1 5 17:00:59 1 5 17:01:05 1 7 19:11:42 1 7 19:11:47 1 7 19:11:55 1 7 19:13:04 1 7 19:13:08 1 7 19:13:11 1 7 19:21:23 1 7 19:21:26 1 7 19:21:31 1 7 19:22:56 1 suspect.log 1 tmp banned.log 192.168.0.18 21:04:50 20:53:55(-)root@datacomm-17:COMP8006_a3$ iptables -L -n Chain INPUT (policy ACCEPT) target prot opt source destination DROP all -- 0.0.0.0/0 192.168.0.18 Chain FORWARD (policy ACCEPT) target prot opt source destination Chain OUTPUT (policy ACCEPT) target prot opt source destination DROP all -- 0.0.0.0/0 192.168.0.18 20:54:11(-)root@datacomm-17:COMP8006_a3$	**PASS**

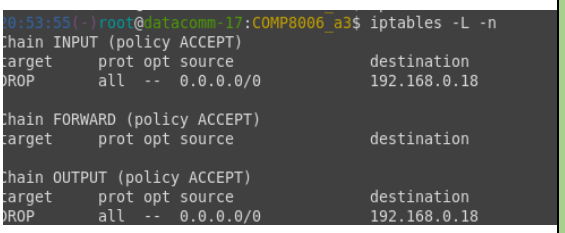
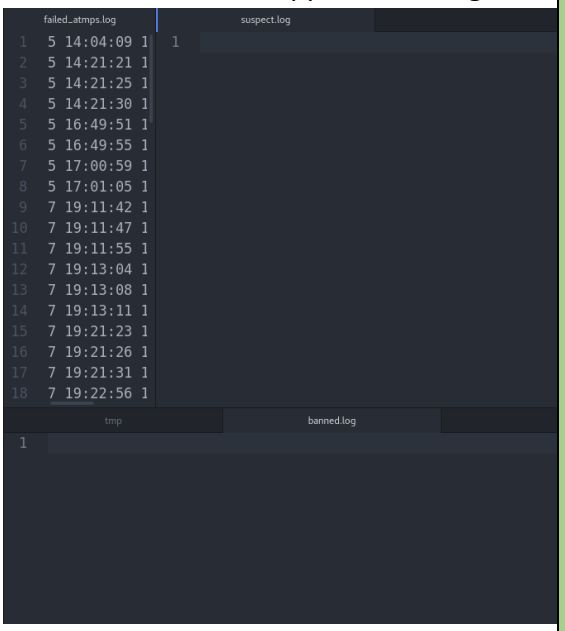
Client banned

```
20:52:32(-)root@datacomm-18:~$ ssh 192.168.0.17
root@192.168.0.17's password:
Permission denied, please try again.
root@192.168.0.17's password:
Permission denied, please try again.
root@192.168.0.17's password:
```

IP is banned after incorrect attempt limit reached (2 tries)

Test Case #9	Expected	Screenshot(s)	Result
Steps: 1. Run the client program as follows on one computer **./ips.sh 1 1 1 1** 2. Find the IP of the client computer by typing in terminal the following command **./ifconfig** 3. On another computer, run the following command in terminal **ssh *ip*** Note: IP indicates the IP of the client computer found in step 2 4. Type in an ***incorrect*** password **one time** 5. Attempt to login with correct password 6. Notice the message displayed on second computer.	User can successfully run the program with no errors. The IP of the computer is found, and user is displayed incorrect password message after attempting to SSH into client with wrong password. After the first incorrect attempt, user's IP is banned and cannot login even with correct password. Check the Suspect file in the COMP8006_a3 folder to ensure IP is banned. Check IP tables to ensure IP is banned.	Server 20:53:57(-)root@datacomm-17:COMP8006_a3$ ./ips.sh 2 0 0 10 Log Files suspect.log 1 192.168.0.18 1 2 failed_atmps.log 1 5 14:04:09 1 2 5 14:21:21 1 3 5 14:21:25 1 4 5 14:21:30 1 5 5 16:49:51 1 6 5 16:49:55 1 7 5 17:00:59 1 8 5 17:01:05 1 9 7 19:11:42 1 10 7 19:11:47 1 11 7 19:11:55 1 12 7 19:13:04 1 13 7 19:13:08 1 14 7 19:13:11 1 15 7 19:21:23 1 16 7 19:21:26 1 17 7 19:21:31 1 18 7 19:22:56 1 suspect.log 1 tmp banned.log 1 192.168.0.18 21:04:50 2 20:53:55(-)root@datacomm-17:COMP8006_a3$ iptables -L -n Chain INPUT (policy ACCEPT) target prot opt source destination DROP all -- 0.0.0.0/0 192.168.0.18 Chain FORWARD (policy ACCEPT) target prot opt source destination Chain OUTPUT (policy ACCEPT) target prot opt source destination DROP all -- 0.0.0.0/0 192.168.0.18 20:54:11(-)root@datacomm-17:COMP8006_a3$ Client Banned 20:52:32(-)root@datacomm-18:~$ ssh 192.168.0.17 root@192.168.0.17's password: Permission denied, please try again. root@192.168.0.17's password: Permission denied, please try again. root@192.168.0.17's password:	**PASS**

IP is allowed after time limit indicated by user is reached (1 minute 1 second)

Test Case #10	Expected	Screenshot(s)	Result
Steps: 1. Run the client program as follows on one computer **./ips.sh 0 1 1 1** 2. Find the IP of the client computer by typing in terminal the following command **./ifconfig** 3. On another computer, run the following command in terminal **ssh *ip*** Note: IP indicates the IP of the client computer found in step 2 4. Type in an ***incorrect*** password **one time** 5. Attempt to login with correct password 6. User is denied entry. 7. Wait at least 1 minute and 1 second, then try again 8. Notice the terminal output on second computer.	User can successfully run the program with no errors. The IP of the computer is found, and user is displayed incorrect password message after attempting to SSH into client with wrong password. After the first incorrect attempt, user's IP is banned and cannot login even with correct password. After a minute and one second, user can ***successfully*** *SSH into computer with correct password.*	Server 1 minute 1 second after 2 tries  Banned IP at first  Unbanned IPs disappear from logs 	**PASS**

IP is allowed after time limit indicated by user is reached (30 seconds)

Test Case #11	Expected	Screenshot(s)	Result
Steps: 1. Run the client program as follows on one computer **./ips.sh 0 0 30** 2. Find the IP of the client computer by typing in terminal the following command **./ifconfig** 3. On another computer, run the following command in terminal **ssh *ip*** Note: IP indicates the IP of the client computer found in step 2 4. Type in an ***<u>incorrect</u>*** password **one time** 5. Attempt to login with correct password 6. User is denied entry. 7. Wait at least 1 minute and 1 second, then try again 8. Notice the terminal output on second computer.	User can successfully run the program with no errors. The IP of the computer is found, and user is displayed incorrect password message after attempting to SSH into client with wrong password. After the first incorrect attempt, user's IP is banned and cannot login even with correct password. After **thirty seconds,** user can log back in with correct password and is not banned.	Server 30 seconds after 2 tries 21:16:59(-)root@datacomm-17:COMP8006_a3$ ./ips.sh 2 0 0 30 Banned IP at first 10:53:55(-)root@datacomm-17:COMP8006_a3$ iptables -L -n Chain INPUT (policy ACCEPT) target prot opt source destination DROP all -- 0.0.0.0/0 192.168.0.18 Chain FORWARD (policy ACCEPT) target prot opt source destination Chain OUTPUT (policy ACCEPT) target prot opt source destination DROP all -- 0.0.0.0/0 192.168.0.18 Unbanned IPs disappear from logs failed_atmps.log 5 14:04:09 1 5 14:21:21 1 5 14:21:25 1 5 14:21:30 1 5 16:49:51 1 5 16:49:55 1 5 17:00:59 1 5 17:01:05 1 7 19:11:42 1 7 19:11:47 1 7 19:11:55 1 7 19:13:04 1 7 19:13:08 1 7 19:13:11 1 7 19:21:23 1 7 19:21:26 1 7 19:21:31 1 7 19:22:56 1 suspect.log tmp banned.log	**PASS**