COMP 8006 Assignment 3 Testing

Alex Zielinski

Contents

Testing Explained	3
Test Cases	3

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

T	est Case #1	Expected	Screenshot(s)	Result
Ste	eps:	Error will pop		
1.	Run the client	up indicate the		
	program as	programs		
	follows	usage.	File Edit View Search Terminal Help	DAGG
	./ips.sh		20:31:07(-)root@datacomm-17:COMP8006_a3\$./ips.sh Usage: ./ips.sh <attempts> <hour> <min> <sec> 20:31:10(-)root@datacomm-17:COMP8006_a3\$ ■</sec></min></hour></attempts>	PASS
2.	Notice the terminal output			

Incorrect user arguments (1)

Test Case #2	Expected	Screenshot(s)	Result
Steps: 1. Run the client program as follows ./ips.sh 1	Error will pop up indicate the programs usage.	20:31:10(-)root@datacomm-17:COMP8006_a3\$./ips.sh 1 Usage: ./ips.sh <attempts> <hour> <min> <sec> 20:31:49(-)root@datacomm-17:COMP8006_a3\$</sec></min></hour></attempts>	PASS
2. Run the client program as follows			

Incorrect user arguments (2)

Т	est Case #3	Expected	Screenshot(s)	Result
Ste	ps:	Error will pop		
1.	Run the client	up indicate the		
	program as	programs	20:31:49(-)root@datacomm-17:COMP8006 a3\$./ips.sh 1 1	
	follows	usage.	Usage: ./ips.sh <attempts> <hour> <min> <sec> 20:32:23(-)root@datacomm-17:COMP8006_a3\$</sec></min></hour></attempts>	
	./ips.sh 1 1			PASS
3.	Notice the terminal output			

Incorrect user arguments (3)

Т	est Case #4	Expected	Screenshot(s)	Result
Ste	ps: Run the client	Error will pop up indicate the		
1.	program as follows ./ips.sh 1 1 1	programs usage.	70:32:23(-)root@datacomm-12:COMP8806 a3\$./ips.sh 1 1 1 Usage: ./ips.sh <attempts> <hour> <min> <sec> 20:32:50(-)root@datacomm-17:COMP8806_a3\$ ■</sec></min></hour></attempts>	PASS
4.	Notice the terminal output			

Correct user arguments inputted

Test Case #5	Expected	Screenshot(s)	Result
Steps: 1. Run the client program as follows	Terminal indicates that program has started. Program is running correctly.	21:16:31(-)root@datacomm-17:COMP8006_a3\$./ips.sh 2 0 1 1	
./ips.sh 1 1 1 4			
2. Notice the terminal output			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	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.	20:30:22(-)root@litecom lo:-\$ ssh 192.168.0.17 rootg192.168.0.17's password: Last failed login: Wed Mar 7 20:30:22 PST 2018 from 192.168.0.18 on ssh:notty There were 31 failed login attempts since the last successful login. Last login: Tue Mar 6 18:33:51_2018 from 192.168.0.16	PASS

SSH into computer with incorrect password

Steps: 1. Run the client program as follows on one computer one computer Jips.sh 1114 2. Find the IP of the client computer by typing in terminal the following command Jifconfig 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. Suspect log file suspect log in a lincorrect password 1. Suspect log file suspect log file should have entry of second computer. Suspect log file should have entry of IP. PASS PASS	Test Case #7	Expected	Screenshot(s)	Result
	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	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	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 Log files Log files 10:24:30 192.168.0.18 11:20:24:36 192.168.0.18 11:20:25:49 192.168.0.18 11:20:25:49 192.168.0.18 11:20:26:56 192.168.0.18 11:20:26:56 192.168.0.18 11:20:20:30:16 192.168.0.18 11:20:20:30:16 192.168.0.18 12:20:30:16 192.168.0.18 13:20:30:22 192.168.0.18 14:20:36:59 192.168.0.18 15:20:37:28 192.168.0.18 16:20:37:38 192.168.0.18 17:20:37:38 192.168.0.18 18:20:37:38:20 192.168.0.18 18:20:38:20 192.168.0.18 20:38:20 192.168.0.18 20:38:20 192.168.0.18	PASS

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

		Sevenehet/s)	Dogult
Test Case #8	Expected	Screenshot(s)	Result
Steps:	User can	Log Files	
1. Run the client	successfully run	failed_atmps.log	
program as follows on	the program with	33 7 20:24:30 192.168.0.18	
one computer	no errors. The IP	34 7 20:24:36 192.168.0.18	
./ips.sh 1 1 1 4	of the computer is	35 7 20:25:49 192.168.0.18 36 7 20:26:56 192.168.0.18	
	found, and user is	37 7 20:30:12 192.168.0.18	
2. Find the IP of the	displayed	38 7 20:30:16 192.168.0.18	
client computer by	incorrect	39 7 20:30:22 192.168.0.18 40 7 20:36:55 192.168.0.18	
typing in terminal the	password	40 7 20:36:55 192.168.0.18 41 7 20:36:59 192.168.0.18	
following command	message after	42 7 20:37:28 192.168.0.18	
/· C C .	attempting to SSH	43 7 20:37:35 192.168.0.18	PASS
./ifconfig	into client with	44 7 20:37:38 192.168.0.18	FASS
	wrong password.	45 7 20:38:00 192.168.0.18 46 7 20:38:04 192.168.0.18	
3. On another computer, run the	After four	47 7 20:38:14 192.168.0.18	
following command in	attempts, user's IP	48 7 20:38:17 192.168.0.18	
terminal	is banned and	49 7 20:38:20 192.168.0.18	
	cannot login even		
ssh <i>ip</i>	with correct	suspect.log	
Note: IP indicates the IP	password.	1 192.168.0.18 1	
of the client computer		2	
found in step 2	Failed attempt		
	logs show correct		
4. Type in an	IP attempting to	failed_atmps.log suspect.log 1 5 14:04:09 1 1	
<u>incorrect</u> password	connect	2 5 14:21:21 1 3 5 14:21:25 1	
<u>four times</u>	Check the Suspect	4 5 14:21:30 1 5 5 16:49:51 1	
	file in the	6 5 16:49:55 1	
F A	COMP8006_a3	8 5 17:01:05 1	
5. Attempt to login	folder to ensure IP	9 7 19:11:42 1 10 7 19:11:47 1	
with correct password	is banned.	11 7 19:11:55 1 12 7 19:13:04 1	
c N ii il	is baililed.	13 7 19:13:08 1 14 7 19:13:11 1	
6. Notice the		15 7 19:21:23 1	
message displayed on		16 7 19:21:26 1 17 7 19:21:31 1	
second computer.	Check IP tables to	18 7 19:22:56 1 tmp banned.log	
	ensure IP is	1 192.168.0.18 21:04:50	
	banned.	2	
		30.52.55()reat@lstycom 17.60MDDDG and intable	
		20:53:55(-)root@datacomm-17:COMP8006_a3\$ iptables -L -n Chain INPUT (policy ACCEPT)	
	Check Ban file to	target prot opt source destination DROP all 0.0.0.0/0 192.168.0.18	
	ensure IP is in ban	Chain FORWARD (policy ACCEPT)	
	file.	target prot opt source destination	
	ille.	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:

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	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.	Server 20:53:57(-)root@ stacomm-17:COMP8806_a3\$./ips.sh 2 0 0 10 Log Files suspect.log 1	PASS
4. Type in an incorrect password one time	Check the Suspect file in the COMP8006_a3 folder to ensure IP is banned.	timp bannedlog 1 192.168.0.18 21:04:50 2 20:53:55(-)root@latacomm-1/: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	
5. Attempt to login with correct password6. Notice the message displayed on	Check IP tables to ensure IP is banned.	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@ atacomm-17:COMP8006_a3\$	
second computer.		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 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	User can successfully run the program with no errors. The IP of the computer is	Server 1 minute 1 second after 2 tries 21:16:31(-)root@datacomm-17:COMP8006_a3\$./ips.sh 2 0 1 1	
2. Find the IP of the client computer by typing in terminal the following command	found, and user is displayed incorrect password message after attempting to SSH into client with	Banned IP at first 10:53:55(-)root@lataccomm=17:COMP8006_a3\$ iptables -L -n Thain INPUT (policy ACCEPT) Target prot opt source destination DROP all 0.0.0.0/0 192.168.0.18	PASS
./ifconfig 3. On another computer, run the	wrong password. After the first incorrect attempt, user's IP is banned and cannot login	Chain FORWARD (policy ACCEPT) carget prot opt source destination Chain OUTPUT (policy ACCEPT) carget prot opt source destination DROP all 0.0.0.0/0 192.168.0.18	
following command in terminal ssh ip	even with correct password. After a minute and one second, user can	Unbanned IPs disappear from logs faled_atmps log 1 5 14:04:09 1 1 2 5 14:21:21 1 3 5 14:21:25 1 4 5 14:21:30 1	
Note: IP indicates the IP of the client computer found in step 2 4. Type in an	successfully SSH into computer with correct password.	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	
incorrect password one time5. Attempt to login		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	
with correct password 6. User is denied entry.		1	
7. Wait at least 1 minute and 1 second, then try again			
8. Notice the terminal output on second computer.			

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	User can successfully run the program with no errors. The IP of the computer is found, and user	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 Thain INPUT (policy ACCEPT) target prot opt source destination prop all 0.0.0.0/0 192.168.0.18	
client computer by typing in terminal the following command	is displayed incorrect password message after	Thain FORWARD (policy ACCEPT) target prot opt source destination Thain OUTPUT (policy ACCEPT) target prot opt source destination DROP all 0.0.0.0/0 192.168.0.18	PASS
./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	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	Unbanned IPs disappear from logs Talled_atmps.log	
5. Attempt to login with correct password6. User is denied entry.7. Wait at least 1	password and is not banned.	tmp banned log	
minute and 1 second, then try again 8. Notice the terminal			
output on second computer.			