Backdoor Assignment

Testing Document

Ian Lee and Luke Tao

Assignment 2 for COMP 8505

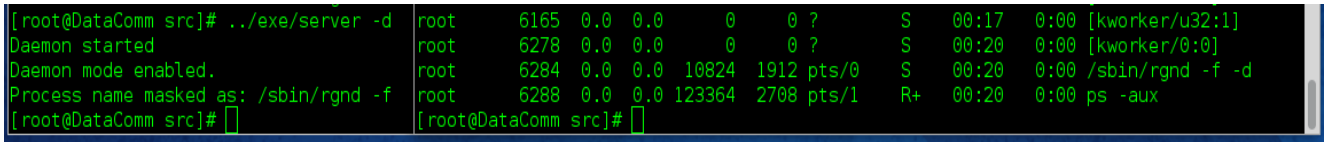
October 6, 2014

Test Case Table

#	Description	Tool	Expected Output	Pass/ Fail
1	Masks Backdoor Process	ps	backdoor renamed	Pass
2	Validates Password	Client	works on matching password; fails on non matching password	Pass
3	Encrypts Payloads	wireshark	unable to read payloads of packets	Pass
4	Commands are executed on backdoor host	touch a file	file is created on backdoor host	Pass
5	Command results are sent back to Client	Client	Results are shown on screen	Pass

Test Case #1

In this test case, we show that the process is masked.



In the screenshot above, the process is renamed to ‘/sibn/rgnd -f -d’

Test Case #2

Here, you can see that when a client enters the wrong password “asdfjkl;”, they get no command results back from the server. However, when the client enters the right password “uest1onQ?”, they should be able to get the results back (see test case #3 for proof).

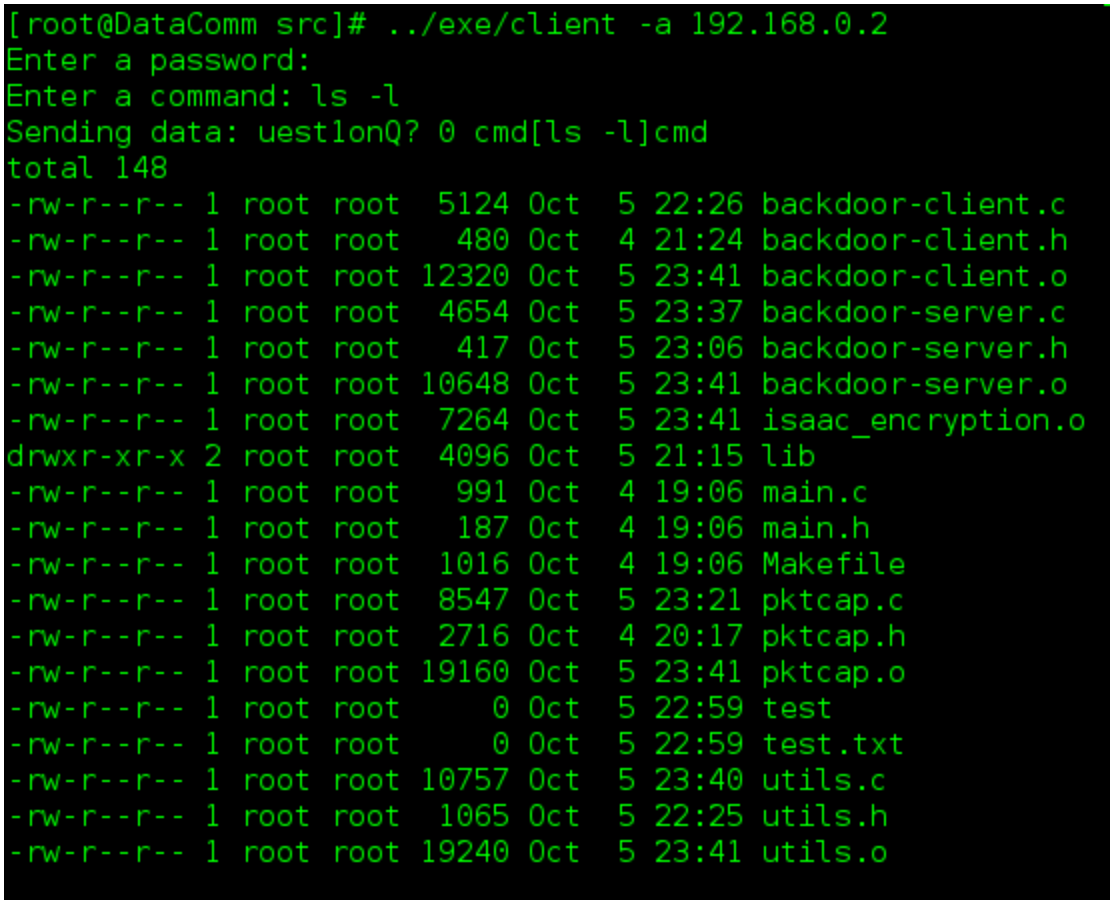
```
[root@DataComm src]# ../exe/client -a 192.168.0.2
Enter a password:
Enter a command: ls -l
Sending data: asdfjkl; 0 cmd[ls -l]cmd

Enter a command: ^C
[root@DataComm src]# ../exe/client -a 192.168.0.2
Enter a password:
Enter a command: ls -l
Sending data: uest1onQ? 0 cmd[ls -l]cmd
```

In the following screenshot, the server recieves an incorrect password and ignores the packet, and a packet with the correct password, and executes it.

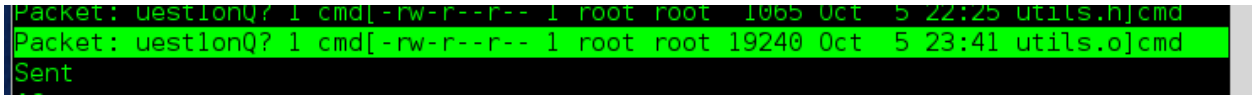
```
[root@DataComm src]# ../exe/server
Daemon mode disabled.
Process name masked as: /sbin/rgnd -f
Incorrect Password
Password Authenticated. Executing command.
Packet: uest1onQ? 1 cmd[total 148]cmd
Packet: uest1onQ? 1 cmd[-rw-r--r-- 1 root root  5418 Oct  5 23:44 backdoor-clien
t.c]cmd
```

Test Case #3

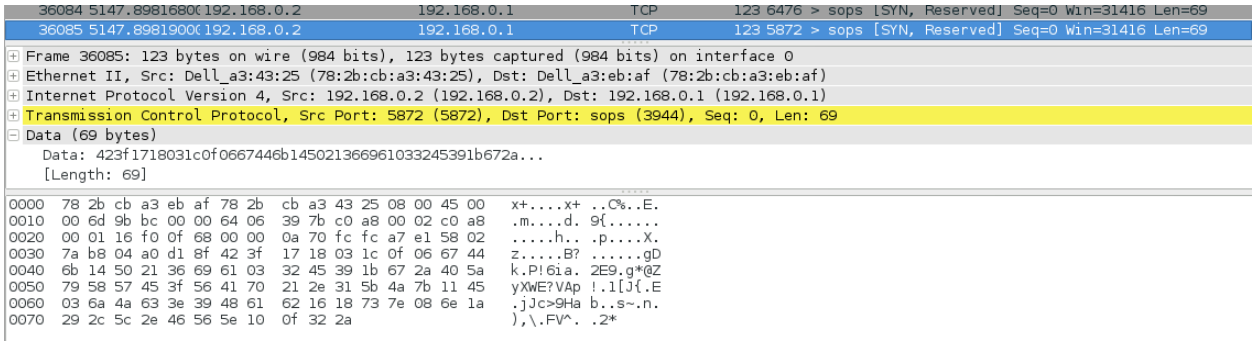
This screenshot shows after the client decrypts the command line results using the XOR algorithm, it displays properly.



For encryption, this packet below shows the command result being sent back to the client.



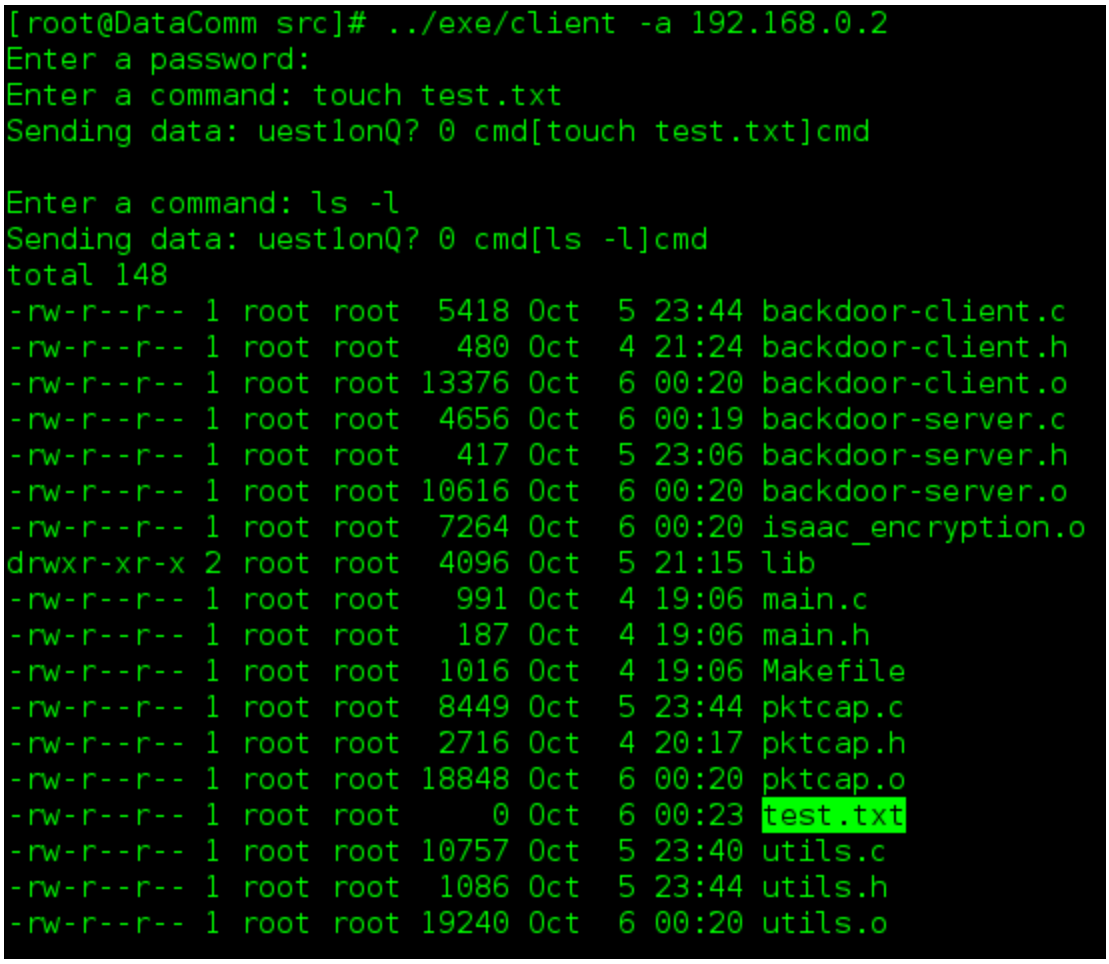
This screenshot in Wireshark shows the same command result mentioned above being encrypted:



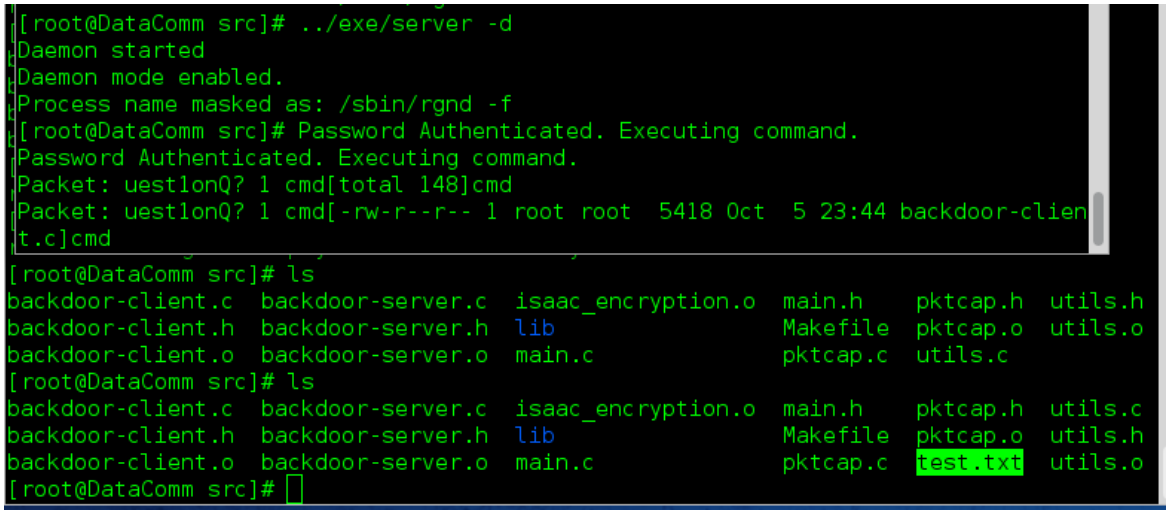
Test Case #4

In this test case we will try to create a file using the command ‘touch test.txt’. To verify that the file is created on the server, ls will be used.

Client side:



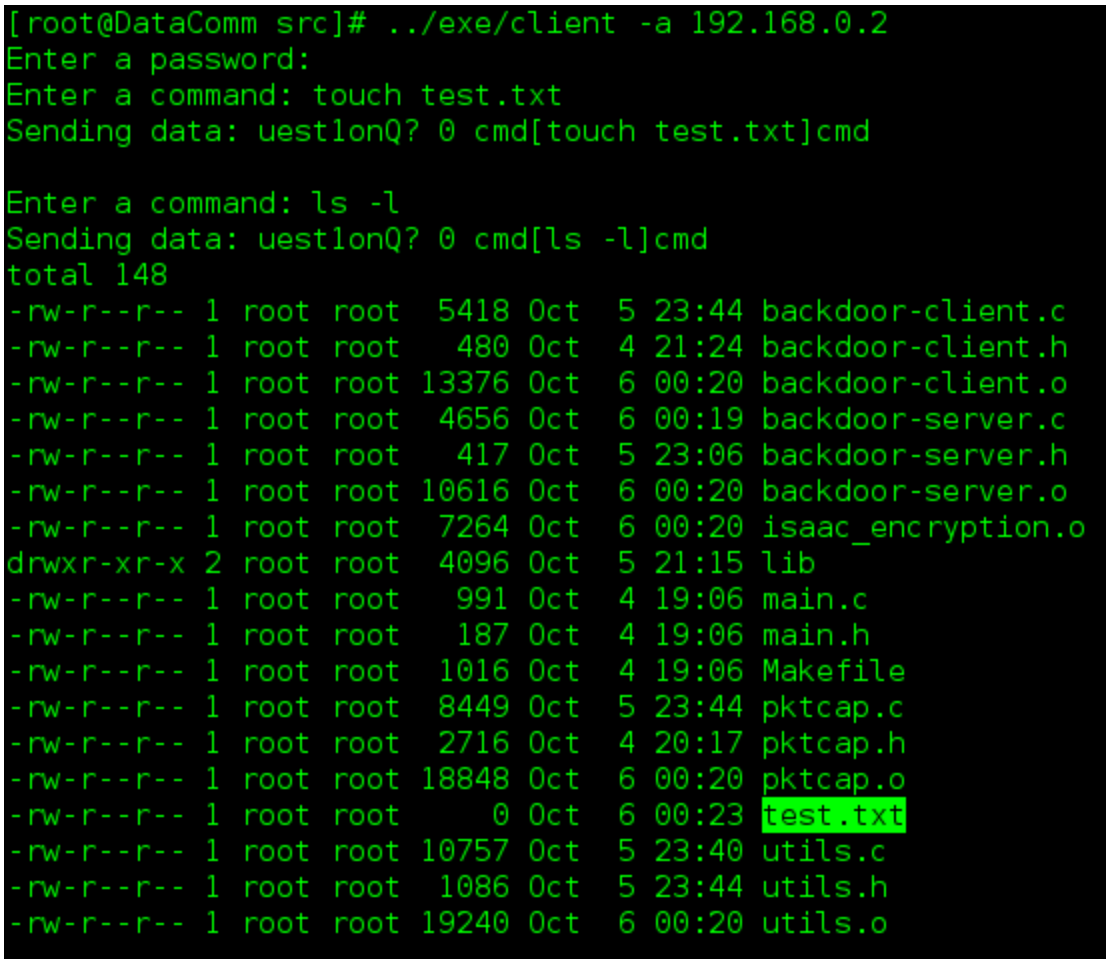
Server Side:



As seen in the screenshots above, the file test.txt was created on the server.

Test Case #5

In this test case, we will check to see that the results of a command, ‘ls’, is returned to the client.



As seen in the screenshot above, the results of ls -l is printed on the client.