CSSE 341 -- Network Security

Rose-Hulman Institute of Technology

Lab 08: Reverse Shell

Learning Objectives

At the end of this lab, you should be able to:

- Define how input and output redirection works in Linux.
- Create TCP connection without specifically creating a server.
- Explore creating a reverse shell in Linux over a TCP connection.

Name: _____

Question	Points	Score
Question 1	5	
Question 2	5	
Question 3	5	
Question 4	5	
Question 5	5	
Question 6	5	
Question 7	5	
Question 8	5	
Question 9	5	
Question 10	5	
Question 11	10	
Question 12	10	
Question 13	5	
Question 14	5	
Question 15	0	
Total:	80	

1 Experiment 1

The questions below refer to `experiment 1`.

Question 1. (5 points) Where do you think `/dev/pts/1` points to?

Hint: Think of the normal behavior of any program, where do you read input from, where does your standard output and error go to?

2 Experiment 2

The questions below refer to `experiment 2`.

Question 2. (5 points) Where is `stdin` mapped for the process?

Question 3. (5 points) What do you think the `0<` syntax did when running `simple_loop.bin`?

3 Experiment 3

The questions below refer to `experiment 3`.

Question 4. (5 points) Before you look at the file mappings, examine the content of the file `output.txt`. Based on your observation, what do you think the file mappings should be now?

Question 5. (5 points) By combining you observations from experiments 2 and 3, can you suggest a method to map the standard error (`stderr`) of the process into a separate file?

Hint: Feel free to experiment a bit and check out the mappings using the same techniques we did above.

4 Experiment 4

The questions below refer to `experiment 4`.

Question 6. (5 points) Where are `stdin` and `stdout` mapped in this case?

Question 7. (5 points) Based on that, what you think the syntax `0<&1` is doing?

Question 8. (5 points) Can you suggest a command that will redirect all `stdin`, `stdout`, and `stderr` to the same file (e.g., `output.txt`)?

5 Experiment 5

The questions below refer to `experiment 5`.

Question 9. (5 points) Explain what the command `echo 'hello' > /dev/tcp/10.10.0.5/9090` did when you ran it? What do you think is the use of the `/dev/tcp` pseudo file?

6 Experiment 6

The questions below refer to `experiment 6`.

Question 10. (5 points) Before you test any commands, where do you expect the output of your commands to show up?

7 Reverse Shell

The questions below refer to the final experiment.

Question 11. (10 points) Write down the command you used to establish a client root shell on the server container.

Question 12. (10 points) Briefly explain (in two sentences) exactly what the command you suggested seems to be doing.

Question 13. (5 points) In your own words, please write a quick summary of what you have learned in this lab.

Question 14. (5 points) How much time did it take you to complete this lab?

Question 15. Do you have any feedback about this lab? (If you'd like to leave an anonymous feedback, feel free to detach this page and slide it under my door).