PenTest Lab Exercise Ex070 – Brian's Service

Goal

Exploit a buffer-vulnerable program. Use fuzz testing and make logical inferences.

Tasks

1. Brian Oppenheimer, son of `artstailor.com` system administrator Otto Oppenheimer, is a budding computer programmer. He posted the following message on the 42chan imageboard just this week:

   > `I am joining the ranks of the 1337 since my dad gave me an account on his company's web server I wrote a service to help sys admins see what's going on with their servers without logging in. It's cool. You can connect to it with netcat and run ps auxww or ip a or netsat -nat. Of course, to keep people from abusing it, I require a username and have inserted other security features.`
   > `-- brian@artstailor.com`

2. Log in to the Netlab server, schedule the PenTest Ex070 Lab, start up the lab, and login to your Kali VM.

3. Perform an `nmap` scan on `www.artstailor.com` to check out Brian's claim. If what he's saying is true, the service should be running there. If you don't notice any ports that seem to implement this service, make sure you scan all available TCP ports to find it.

4. If you're not familiar with `netcat` (the `nc` command), then `nc -h` is your friend.

5. See if you can find a way to exploit a vulnerability in Brian's code to get shell access. You'll need to do this by manually fuzz-testing it, that is providing intentionally wrong inputs in order to get it to do something unintended. You'll also need to correctly infer how to execute a shell command on host `www.artstailor.com`. Make sure to explain how you identified this problem in your report.

6. If you can exploit this program, try to find its source code and identify what problem in the program caused it to fail. Briefly explain that problem in your report.

7. Write a brief report discussing the findings associated with the vulnerability that you identified and exploited. Explain the fuzz testing you did and how it led to exploitation.

8. And yes, a key is available if you succeed. You may be able to find out other useful information by looking around on this server. But remember, system configurations change over time.