Exercises:

July 12, 2021

1 Establishing TCP and UDP connections

Now we are going to test the commands from here. Since we are not running a server anywhere, we will be connecting to localhost. (the -v option is your friend!)

1.1 Tell netcat to listen on a specific port on your machine

1.2 Open a second terminal, then try the portscan command from the link above on your localhost!

Make sure it's your localhost you are scanning, not everyone likes there servers being scanned. Notice what happens in the terminal that was hosting

1.3 Set up your 'server' so it will transfer information into the 'semester' file in the missing directory

Note: If you located the semester file in the /tmp folder last time, it have likely been deleted by now since the folder gets cleaned up regularly. In that case just create a new file, it's not important where it is going.

2 Binding shells, reverse shells

Taken from here, we are going to simulate an attack on ourselves.

2.1 Set up your 'server' to execute bash commands

2.2 Connect to the 'server' using netcat, then find and delete the semester file from earlier through the connection

Close the connection once you're done.

2.3 Now setup 'your own machine' to be ready to receive a reverse shell, then connect with the 'server'

3 Bonus exercises: CTF training game

If you feel like more you can try out the challenges found at OverTheWire. The bandit challenges linked involves you connecting to a server and locating the password for the next level on it. The first 9 levels should be doable for you at present, with the tips provided on the site, but feel free to do more if you find them interesting. You connect to the server using the below command, where userename is the name of the level, e.g. bandit0, bandit1 etc.

```
ssh -p 2220 username@bandit.labs.overthewire.org
```

Once you are connected to this server don't worry about accidentally breaking something, you can't.