Network scanner

The main goal is, to get an understanding of how a 3-way handshake works, and how we can use this knowledge to detect if there is a system running, as well as which services is running on the machine.

Introduction to python

1) Write a small script, where you make a loop that iterates 100 times. For every iteration, print out the number of iteration to the console.
2) Write a script that reads to arguments (e.g. python main.py **arg1 arg2**) and prints out the arguments to the console.
3) Write a small script that has a function called "add_them_numbers". The function should take two parameters and return the sum of the two. Call the function and write the result to the console.
4) Make a script that combines the three upper tasks. The script should take two arguments, make a loop that iterates 100 times, and for every time it iterates call a function that adds the two arguments to each other. Save the result for every function call in an array. After all the iterations, make a sum of the array and print it to the console.

Network scanner

For this exercise, we are going to build a network/port scanner similar too Nmap (just a more simplified). To do this, we will be using Scapy to produce some TCP/IP Packages, and use our knowledge about the 3-way handshake to make the magic work.

1) The scanner should hold a list of different ports that you wish to scan, and take that address it should scan, as an argument.
2) Make the scanner a "Stealth scanner".
3) Expand the scanner, so you can give the port range as an argument.