**Lab 1: Discovery - the host**

**Overview:**

In this lab, we will discover what services are available on our hosts and write-up the results. We will do this discovery with a number of different commands.

**Objective:**

1. Learning to use the ‘netstat’ and ‘lsof’ commands
2. Learning to use one of more commands that replace ‘netstat’
3. Learning to compare commands

**Note:**

In addition to your Linux host, you will need a Window’s host for this lab. If you do not already have one running, put one in place.

**Part 1: What is listening on the local host**

Here we are looking at our hosts to see what services they are running.

In each of the following readings, **try the examples** and **record which services are running, the ports they are listening to, their states, etc.**

Both Unix and Microsoft OSs have a command called netstat, which allows us to analyze our network connections.  
  
Read [this article](http://en.wikipedia.org/wiki/Netstat) to get a quick understanding of the netstat command.   
  
Read [this article](http://commandwindows.com/netstat.htm) to get an introduction to netstat in Windows.   
  
Read [this article](http://www.cyberciti.biz/faq/find-out-which-service-listening-specific-port/) to get an introduction to netstat and lsof in Linux.  
  
[Efficient CLI netstat use.](http://www.simplehelp.net/2009/01/19/monitor-your-linux-machine-with-netstat/)  
  
[Here are some interesting things](http://www.cyberciti.biz/tips/netstat-command-tutorial-examples.html) you can do with netstat in Linux.  
  
By now you should know which network services are running on both Windows and your Kali install.  
  
If you are going to be a security expert, it is imperative that you understand network troubleshooting. Familiarize yourself with the Linux tools discussed [here](http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch04_:_Simple_Network_Troubleshooting" \l "Testing_Your_NIC). See if you can find Windows equivalents for each of these tools.

**Part 2: What is listening on the local host**

As often happens commands can be deprecated and the ‘netstat’ command is no exception to this and has be largely replaced been replaced by ‘ss’ on Linux.

For the Linux ‘netstat’ examples you did in **Part 1** find the equivalent ‘ss’ command. Be warned, you made need to use one or more commands other than ‘ss’ to get the results of a single ‘netstat’ example.

**Lab Write-up Format:**

Your lab should be written up in a document with the following format:

**Title:** Lab 1

**Name:** <your name>

**Student ID:** <your student number>

**Part 1: netstat and lsof**

<command example>

<results>

<command example>

<results>

**Part 2: SS and other commands**

<netstat command example> -- just the command and not the results

<your ss command>

<your ss command results>

NB: if you needed to you use two or more commands to achieve the results of one netstat command, you to include all the commands used and their results

<netstat command example> -- just the command and not the results

<your ss command>

<your ss command results>

**Deliverable**

Submit your results file in ‘.docx’ through the course’s Moodle site with the following name

* LearnName\_Lab1.docx

NB:

* Files not submitted in the .’docx’ format will NOT be marked.
* Submissions deadlines are given through the lab submission link.