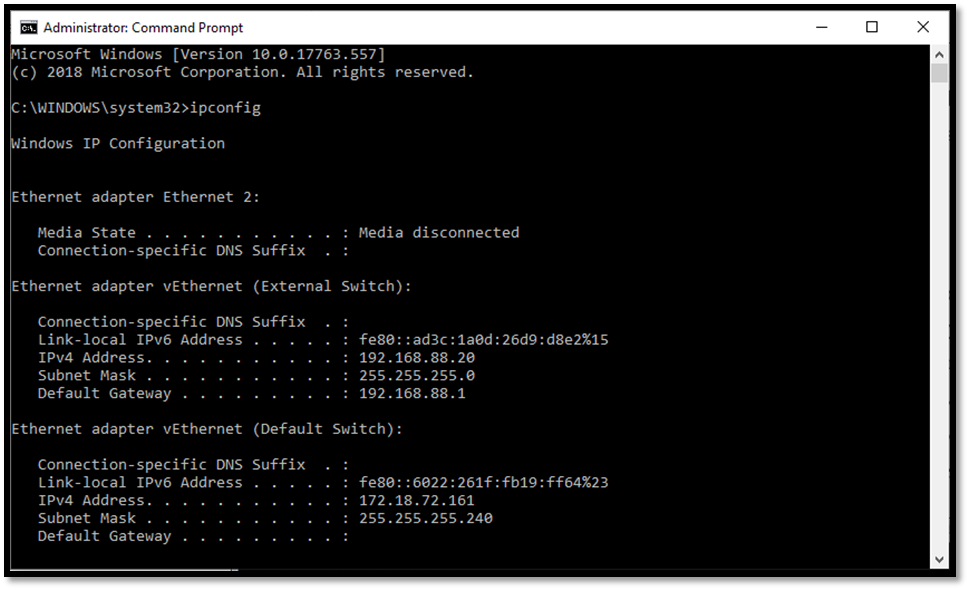
# **1.4 Basic Network Utilities**

Now that you know what IP addresses and URLs are, you need to become familiar with some basic network utilities. Certain network utilities can be executed from a command prompt (Windows) or from a shell (Unix/Linux). Many people are already familiar with Windows, so let’s focus on how to execute the commands from the Windows command-prompt perspective. However, these utilities are available in all operating systems.

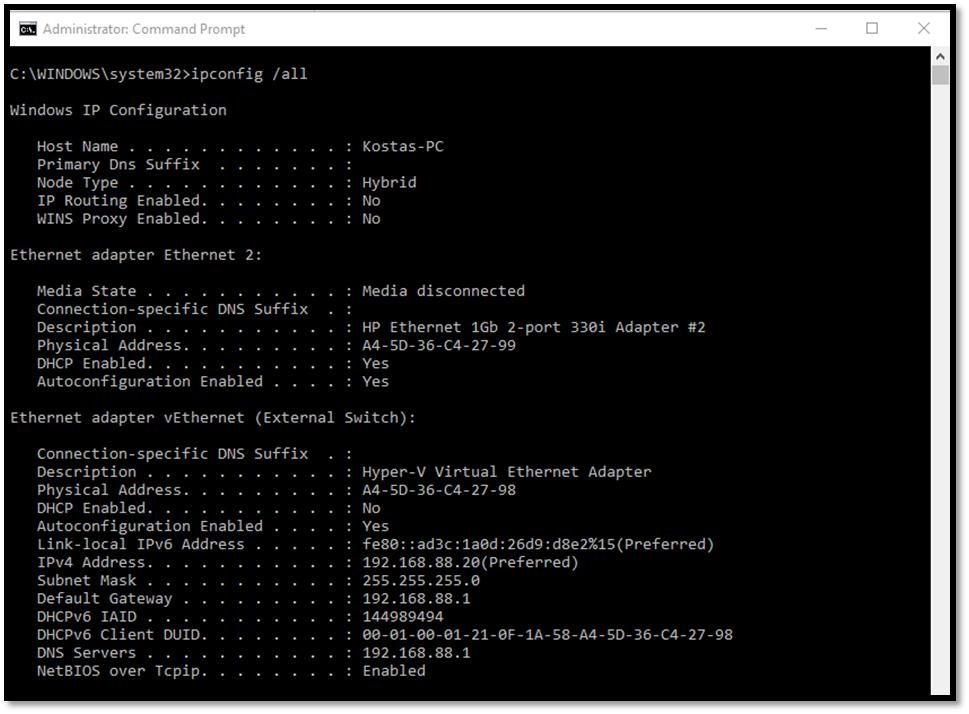
### **1.4.1 Ipconfig**

The first thing you should do is to get information about your own system. To accomplish this, you must get a command prompt. In Windows, you can do this by going to the Start menu, selecting All Programs, and then choosing Accessories. You can also go to Start, Run, and type cmd to get a command prompt. In Windows 10 you must go to Search and type cmd. Now, you should be able to type in ipconfig. (You could input the same command in UNIX or Linux by typing in ipconfig from the shell.) After typing in ipconfig (ipconfig in Linux), you should be able to see something similar to the screenshot below.



This command provides you with information about your connection to a network (or to the Internet). Most importantly, you find out your own IP address. The command also has the IP address for your default gateway, which is your connection to the outside world. Running the ipconfig command is the first step in determining your system’s network configuration. Most commands including ipconfig have a number of parameters, or flags, which can be passed to the commands to make the computer behave in a certain way. You can find out what these commands are by typing in the command, followed by a space, and then typing in hyphen question mark: -?.

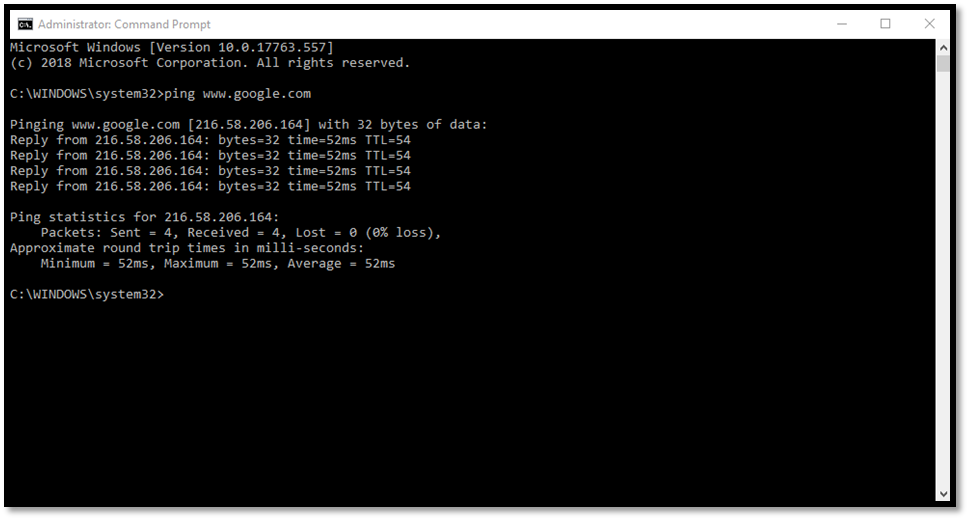
As you can see, you might use a number of options to find out different details about your computer’s configuration. The most commonly used method would probably be ipconfig/all.



### 

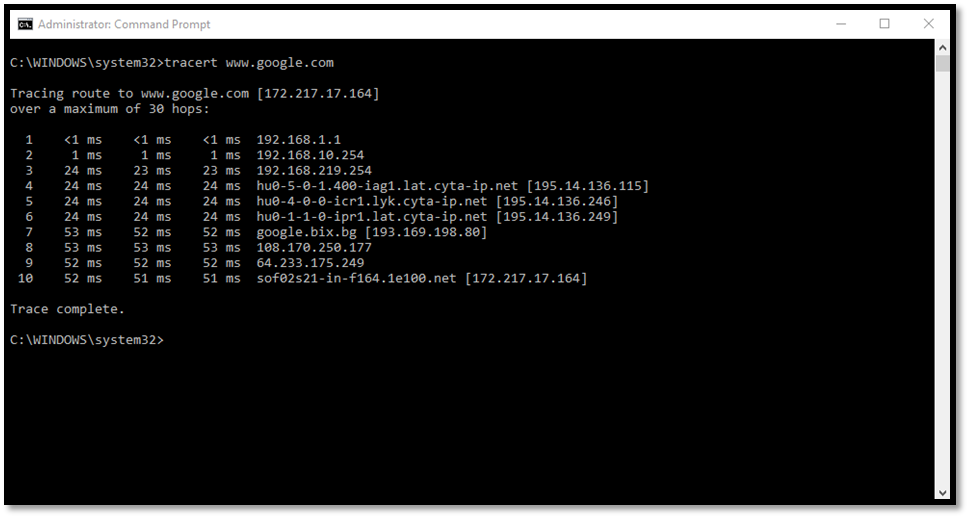
### **1.4.2 Ping**

Another common used command is ping. Ping is used to send a test packet or echo packet, to a machine in order to find out whether the machine is reachable and how long the packet takes to reach the machine. This useful diagnostic tool can be implemented in elementary hacking techniques. Figure 1-3 shows the command.

  
The above command shows that a 32-byte echo packet was sent to the destination and returned. The TTL means “time to live.” That time unit is how many intermediary steps, or hops, the packet should take to the destination before giving up. Remember that the Internet is a vast conglomerate of interconnected networks. Your packet probably won’t go straight to its destination. It will have to take several hops to get there. As with ipconfig, you can type in ping -? to find out various ways you can refine your ping.

### **1.4.3 Tracert**

The next command is tracert. This command is a sort of “ping deluxe.” Tracert does not only inform you whether the packet got there and how long it took, but it also gives you all the necessary information regarding all the intermediate hops it took to get there. (This same command can be executed in Linux or UNIX, but it is called traceroute rather than tracert.) You can see this utility in Figure 1-4.



Tracert enables you to see (in milliseconds) the time that the IP addresses of each intermediate step was listed, and how long it took to get to that step. It is very important to be well versed in the steps required to reach a destination.

### **1.4.4 Netstat**

Netstat is another interesting command. It is an abbreviation for Network Status. Essentially, this command tells you what connections your computer currently has. Don’t panic if you see several connections;This does not mean that someone has hacked your computer. You will see many private IP addresses. This means your network has internal communication going on. You can see this in Figure 1-5.

Certainly, other utilities can be used when working with network communications. However, the four we just examined are the core utilities. These four (ipconfig, ping, tracert, and netstat) are absolutely essential to any network administrator.

