Hidden Site Student Instructions

Introduction:

Welcome to the hidden site workout where you learn how to scan ports to find a hidden service. For this workout you will be utilizing a tool that scan ports like nmap or zenmap and a web browser like Firefox.

Before learning about ports, let's talk about IP addresses.

An IP address is typically a series of numbers that are assigned to a computer connected to a network. An example would be like **192.168.0.1.** Think of IP addresses like a real life street address but for computers.

What's a port?

A port is a networking endpoint that identifies a service or process. What exactly does that mean? Consider an apartment complex or maybe a hotel that has different numbers to identify the rooms. Ports are numbers that are extensions of an IP address. These numbers identify different protocols and services used in a network. For instance, port 20 and 21 refer to FTP or File Transfer protocol. This protocol allows for a user to download and upload files to a server. If you have some extra time, use Google to look up a list of commonly used ports on the Internet. You'll find that you use a number of these services every day without even realizing it.

Your mission:

- Once you are logged in, open up the terminal on your machine.
- Within the terminal, you'll be able to use a variety of tools and commands just by typing it in.
- For this lab, you will be using nmap which stands for network mapper. This tool is used to find open ports on a server.
- The command will look something like this: `nmap 127.0.0.1`
- This will scan the IP address 127.0.0.1 which is your own machine for any open ports. You may have to adjust the IP address depending on how the servers are setup.
- Once, that's done you should be presented with a list of port numbers and their services.
- From here on, you will need to figure out which of these ports contains the hidden web server and the flag.

- Usually, web servers are on port 80 or port 8080, but this time it’s been changed to make it a little harder.
- Open up your web browser like Firefox, and type in something like this in the address box:
- `http://127.0.0.1:80`
- Notice how after the IP address, there’s a colon and then a number. This number signifies the port for that IP address. Change the port in the example with one of the ports on your list. Most of them will probably give you an error or no response at all. One of the ports will tell you that you’ve found the hidden web page with a flag. See if you can find the hidden site.