# Surfing from Starbucks, or Penetration testing through an SSH tunnel

This is a short little exercise, mostly for fun. It would work with either of the two following scenarios.

## Scenario 1, Surfing from Starbucks

You are at Starbucks, or worse yet, the Blackhat convention and you want to surf without worrying about Man in the Middle (MitM) attacks. If you have a trusted remote server that allows SSH and you already have the server’s public key on your laptop so that you know that you are connecting to your server and not some imposter, you can surf through an encrypted SSH tunnel. But, where can you find an SSH server you trust, and where you already have its public key? Hmmm, remember the Cloud VM lab?

## Scenario 2, Penetration testing through an SSH tunnel

You have been hired to test the security of XYZ Company. More importantly, you have a signed document from the company that details what you can do (scope) and gives you permission to do it. You know that the company keeps its crown jewels on the SuperSekret web server, but the server is only accessible by certain computers in the company. However, you have been able to obtain access to one of those “certain computers” and you have put your public key in the ~/.ssh/authorized\_keys file of that computer. Now you can use an SSH tunnel to that computer to browse the SuperSekret web server.

## Hand in

Create a dynamic SSH tunnel to a machine (instance perhaps?) that is not on the SVGS campus. Configure your browser to use that tunnel as a SOCKSv5 proxy, and then surf to other sites using that tunnel.

1. Hand in screenshots of the command you used to create the SSH tunnel, and of the browser proxy configuration.
2. Take a Wireshark packet capture while you are browsing through the tunnel. Identify the traffic in Wireshark that shows you browsing through the tunnel and turn in a screenshot.