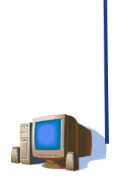
This exercise should be completed in groups of size **3**. Please use only 1 laptop per group.  
  
Obtaining illegitimate access to internal networks may require only a single, vulnerable point of entry. Adversaries exploit vulnerable hosts and use them as stepping stones to bypass firewalls, intrusion detection systems, and other defense mechanisms.

In this exercise, you will learn about the tools and methodologies that attackers use to pivot through networks.

**Your goal is to obtain a password hash file and   
crack 4 passwords**  
While dumpster diving, you were able to obtain the following Figure.

****

**TARGET**

**10.0.0.1**

**10.0.2.2  
pivot point**

**Network Scenario Figure**

# UBER Challenge Hints

***Note: Please ensure that your laptop’s wireless interface is turned off***

1. You will need to ***closely*** inspect the web page on the web server.

2. Many services set default passwords to the same value as the username.

2. You will need to use your **meterpreter session**; you can go back to your session by executing the following command:

***sessions –i 1***

3. Consult the **help command** within meterpreter to investigate another way to **forward** traffic.

4. You’ll need to use the secure shell, ***ssh***, program to login to a remote device; it uses port 22 by default.

5. Consult the **man page for ssh** (you’ll need to know how to login as a specific user)

6. On Linux operating systems, password hashes are located in following folder:

***/etc/shadow***

7. ***johnny*** is an application in Kali Linux that is used for cracking passwords; it takes a password hash file as input.

**When you’re done, please raise your hand and notify the coordinators.**