# Using nmap for network discovery

This lab was developed for the Labtainer framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations under National Science Foundation Award No. 1438893. 

## Overview

This Labtainer exercise explores the use of the nmap utility to discover computers and services on networks.

## Begining the lab

The lab is started from the labtainer working directory on your Linux host, e.g. , a Linux VM. From there, issue the command:

```
labtainer nmap-discovery
```

The resulting virtual terminal will include a bash shell. The nmap utility is pre-installed on the computer connected to the termial.

## Tasks

Your boss Randall wants you to prepare for a meeting on a project you have not worked on in months. You have a summary file on the "friedshrimp" server that you previously accessed via ssh; however, you cannot remember the IP address of "friedshrimp", and you also forgot which port the pesky IT staff assigned for ssh on that server. You know it's somewhere in between 2000 and 3000. The one thing you most certainly know is that your password is the usual one used in these labs. You are left with only one option: use the nmap command to find the IP address and and port number used by the ssh service. After finding that information review the contents of the "friedshrimp.txt" file from an ssh session.

If you need any help with the nmap commands, you can use "`man nmap`" to view the manual. Note that in order to ssh to a host via a port other than the default one, use "`ssh -p <port> <host>`".

## Stop the labtainer.

When the lab is completed, or you'd like to stop working for a while, run:

```
stoplab
```

from the host Labtainer working directory (VM). You can always restart the Labtainer and continue your work. When the Labtainer is stopped, a zip file is created and copied to a location displayed by the "`stoplab`" command. When the lab is completed, send that zip file to the instructor.