INTRUSION DETECTION v0.1
Assignment 2 - 160 pts (60 pts BONUS)
Due: October 10, 2015 11:59 PM

netsec

Description:
Your task is should you choose to accept is one to detect intruders on our network 'netsec'. Analysts have the information to believe that there is an intruder on the network and we must determine the source as soon as possible.

The intruder intermittently appears on the network and as such it has been hard to detect, in that timing must be precise for us to see them. We have reason to believe that if we set up a program that continuously monitors attached devices MAC addresses we will be able to determine who the intruder is.

Our analysts have shared with us a command they find useful for the work they have done when looking at log files.

grep -Eo '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}'

First, I don't understand what those number guys were getting at so can you put into words what the above means so I can explain it to the rest of the unit?

Next, the way that we have determined to detect the intruder is rather straight forward. If we keep track of the connected users on the network by maintaining a count, increasing for each time we check, we will be able to see which users are commonly connected. Now thing is we know the intruder only intermittently connects, so if we take a look at the data we will see a user that hasn't been on the network as often as the others. That is our intruder.

So first thing is first let's utilize the *nmap* tool to look at our network. You will have to write a script that continuously monitors devices connected counts, or you can write a post processing script to do the counting work for you after the fact (you'll have to log your monitoring output). Implementation details are up to you.

Also before I forget, our analysts have told us that checking IP addresses, like they have been, haven not been helpful since our network is DHCP, and they keep changing as time goes on. So they think you can modify the command the analysts have provided to look for MAC addresses. This should clear up any issues with any IP addresses getting switched around.

If you have any questions refer to the requirements and ask me for any details. You can reach me at jw2772@mcla.edu.

Good Luck!

Requirements:

Deliverable *SHALL* include a description of the analysts grep syntax call. Each part of the syntax, character by character.

Deliverable *SHALL* be a bash script(s) capable of monitoring attached network devices using the tool nmap.

Deliverable *SHALL* log nmap outputs.

Deliverable *SHALL* output to the user the count of times unique MAC addresses have been seen.

Deliverable *SHALL* output to the user the count of times unique IP addresses have been seen.

Deliverable *SHALL* log all IP addresses and MAC addresses on the network.

Deliverable *SHALL* output no errors or warnings.

Deliverable *SHALL* be able to run in any subdirectory within the home subdirectory. (Use relative path names rather than absolute)

BONUS:
(20 pts) Display a histogram or graph associating counts with network devices IP addresses. Can be graphical based or output in command line.

(20 pts) Display a histogram or graph associating counts with network devices MAC addresses. Can be graphical based or output in command line.

(20 pts) In class demonstration of working program.

HINTS:
You will be provided with a log file so that you can develop your script without being on the isolated network. After you determine how to use nmap to monitor the network you will comment out that command and replace it with a cat of the log file. We will go over this in class.