Coding 1

Explanation: This challenges requires the use of a unix machine and knowledge of different commands such as “string” and “md5sum”.

Solution: \*This is one possible solution to the problem\*

In Terminal, navigate to the folder containing the malwareDebug.pcap file. Entering

the following command will return a list of all printable strings in malwareDebug.pcap that are at least 10 consecutive characters long.

# strings -10 malwareDebug.pcap

You can use this list of strings with a bash script using md5sum or (as I did) put the results in a text file as below and use a python script to hash the results and compare with the check given in the prompt.

# strings -10 malwareDebug.pcap >> now.txt

Python:

import hashlib

f = open(‘now.txt’,’r’)

check = 2a918cc5cde616ad48b818176772f029

for line in f:

if hashlib.md5(line.strip()).hexdigest() == check:

print(line)

f.close()

Executing this script as below will print the string that matches the hash.

# python [filename].py

securecentral ←-- matching string

Flag: securecentral