CSC304
Digital Forensics and Incident Response
Lab Exercise 2: Learning Vi

Grading: Not graded but may Be audited class participation

Due Date: Next scheduled class

Purpose

The purpose of this lab exercise is to learn basic **vi** skills. Production servers typically have all software unrelated to its main purpose disabled/uninstalled to minimized the attack surface. The **vi** editor is traditionally the default **cron** editor on all Unix and Linux operating systems. and in fact, it may even be the only editor available. Therefore, knowing **vi** is a necessary IT skill to support forensic investigative processes.

References

There are many online guides for the **vi** editor, ranging from simple beginner's guides to more advanced tutorials. Find one that is suited to your IT experience level and individual learning style. No one size fits all but you can use this as a starting point:

https://www.jics.utk.edu/files/images/csure-reu/PDF-DOC/VI-TUTORIAL.pdf

Download the pdf and save it for future reference.

Lab Task 1:

It is customary to have a warning banner for servers to warn away potential intruders. There is no evidence that warnings of any sort deter determined attackers but it does help form a legal basis for prosecution.

By default, the Kali Linux displays the MOTD file upon logon.

```
┌──(kali㉿kali)-[~]
└─$ ls -l /etc/motd
-rw-r--r-- 1 root root 282 Aug  8 12:35 /etc/motd
```

View the contents of /etc/motd.

ALWAYS make a backup of system files that you are going to modify.

```
$ sudo cp /etc/motd ~/motd.backup
```

Use **vi** to change the contents of /etc/motd to the warning shown below and save it.

```
##################################################################
#                                                                #
#                                                                #
#                            NOTICE                              #
#                                                                #
#             THIS IS A PRIVATE COMPUTER SYSTEM                  #
#  protected by the Budapest Convention on Cybercrime,           #
#  Computer Fraud and Abuse Act, Electronic Communication Act    #
#                 and the USA Patriot Act.                       #
#                                                                #
#          All activities are monitored and logged.              #
#     Evidence of criminal activity will be reported to          #
#          the federal law enforcement authorities.              #
#                                                                #
#      Do not proceed if you are not an authorized user.         #
#                   DISCONNECT IMMEDIATELY                       #
#                                                                #
#                                                                #
##################################################################
```

Confirm that when users access Kali Linux, that they will see a pretty formatted motd like the above.

Questions

Answer these questions and save the answers in a MS Word document under the name Lab_Exercise_1_Y*ourName*.doc. The answer sheet must have the lab title, your name and the date of completion. All lab exercises must be completed on the due date. However, *do not* send the answer sheet. Keep it until it is requested by the instructor.

1) Who is the owner of /etc/motd?
2) Under what circumstances is the content of /etc/motd displayed?
3) How did you confirm the change took effect?
4) What did you learn from this exercise?