# Scripting for Security Lab: Grep

michaelferrie@edinburghcollege.ac.uk

## Part 1: Open Jupyter VM

1.1 Open jupyter vm and log in. We can use this to complete the lab.

## Part 2: The Dictionary

2.1 Have a look at the contents of the dictionary with cat

```
cat /usr/share/dict/words
```

2.2 Now to use some new grep skills, run grep on the dictionary and find any words that contain the letter x

```
grep x /usr/share/dict/words
```

2.2 Find any words in the dictionary stored in /usr/share/dict/words that start with the letter i using the caret ^ symbol:

```
grep '^i’ /usr/share/dict/words
```

2.3 Find any words that end with the letter i using the dollar $ symbol:

```
grep ‘.i$’ /usr/share/dict/words
```

2.4 Find any words in the dictionary stored at /usr/share/dict/words that start with the letter i and end in the letter n that have seven characters.

2.5 How many words end in the letter p?

2.6 How many words contain the phrase ‘polin’?

2.7 How many words start with ‘catti’?

## Part 3: Grep a log file

3.1 Open jupyter and drag the access log file from moodle into the file manager :

3.2 Have a look at the contents of the file using the cat command as demonstrated in step 2.1.

3.3 Grep for every line that starts with 178

3.4 A .(dot or full stop) in a grep command means any character, but if we want to search for a . we need to escape it with \ like this \. Find out how many lines in the access log start with 178.32.

3.5 Pipe the contents of grep into the wc program with -l to get the number of lines, for example: `grep ‘Firefox’ access_log | wc -l.` How many lines contain the word Apple?

3.6 Grep -v gives an inverse search, so you can search for a negative match, using the -v how many lines do not contain the word Apple?