Lab: Hashcat

1 Run the hashcat benchmark (eg hashcat – b -m 0), and complete the following:

Device: Hash rate for MD5: Hash rate for SHA-1: Hash rate for SHA-256: Hash rate for APR1:

2 We have hashed a SHA-256 value of the following and put it into a file named file.txt:

```
106a5842fc5fce6f663176285ed1516dbb1e3d15c05abab12fdca46d60b539b7
```

By adding a word of "help" in a word file of words.txt, prove that the following cracks the hash (where file.txt contains the hashed value):

```
hashcat -m 1400 file.txt words.txt
```

3 The following is an NTLM hash, for "help":

```
0333c27eb4b9401d91fef02a9f74840e
```

Prove that the following can crack the hash (where file.txt contains the hashed value):

```
hashcat -m 1000 file.txt words.txt
```

4 Now crack the following Scottish football teams:

```
635450503029fc2484f1d7eb80da8e25bdc1770e1dd14710c592c8929ba37ee9
b3cb6d04f9ccbf6dfe08f40c11648360ca421f0c531e69f326a72dc7e80a0912
bc5fb9abe8d5e72eb49cf00b3dbd173cbf914835281fadd674d5a2b680e47d50
6ac16a68ac94ca8298c9c2329593a4a4130b6fed2472a98424b7b4019ef1d968
```

Football teams:

5 Rather than use a dictionary, we can use a brute force a hashed password using a lowercase character set:

```
hashcat -a 3 -m 1000 file.txt ?l?l?l?l?l?l?l?l
```

Using this style of command, crack the following words:

```
4dc2159bba05da394c3b94c6f54354db1f1f43b321ac4bbdfc2f658237858c70
0282d9b79f42c74c1550b20ff2dd16aafc3fe5d8ae9a00b2f66996d0ae882775
47c215b5f70eb9c9b4bcb2c027007d6cf38a899f40d1d1da6922e49308b15b69
```

Words: Number of test for each:

6 We can focus on given letters, such as where we add a letter or a digit at the end:

```
hashcat -a 3 -m 1000  file.txt password?l
hashcat -a 3 -m 1000  file.txt  password?d
```

Using these commands, crack the following:

```
f19bd0844e53369373385609e28dbf84
db0edd04aaac4506f7edab03ac855d56
```

Words: Number of tests for each:

7 It is known that a user has used a password of "pass*X*ord", where *X* is an unknown character or number. Can crack the following hashes based on a filter:

e3ccac84b0909e29721b891c11c45d2fceb08018a06512c51577fd912b13a1e7
8f0e2f76e22b43e2855189877e7dc1e1e7d98c226c95db247cd1d547928334a9

Passwords used: Number of tests:

8 Download the bfield.hash password hash, and using the rockyou.txt list, determine the first 10 passwords in the hashed file. An example command might be:

```
hashcat -m 0 bfield.hash /usr/share/wordlists/rockyou.txt
```

First 10 passwords from bfield.hash:

Appendix

User logins:

Ubuntu (User: napier, Password: napier123).
Windows2003 (User: Administrator, Password: napier).
Windows 2008 (User: Administrator, Password: Ankle123).
Pfsense (User: admin, Password: pfsense).
Windows 7 (User: EnCase, Password: napier).
Kali (User: root, Password: toor).