Computing

Lesson 3: Script Kiddies

Cybersecurity

Ben Garside

[1] *Materials from the Teach Computing Curriculum created by the National Centre for Computing Education*

Task 1 - Brute force: Passwords

For this activity you will need to use/run and amend the following python program to be able to answer the questions on the following slides:

oaknat.uk/comp-brute-force

Please ask a parent or carer for permission before attempting this task. Oak National Academy are not responsible for any third party content.

Task 1 - part 1

The program has been set to output how many attempts it took to find the password (set on line 11), as well as how long it took the computer to do it.

Run the program.

Follow the instructions on the next slides and note down the results.

Task 1 - part 2

Instruction	Number of attempts	Time taken (round up to two decimal places)
Run the program with the password ‘ab’		
Change the password to ‘abc’		
Change the password to ‘Abc’		
Change the password to ‘Abc1’		

Task 1 - part 4

The program has been set to check only for ASCII letters and digits.

Modify line 15 of the program so that it checks for punctuation and any white space in the password (white space is an empty value in the password, such as a space).

Line 5 should now look like this:

```
15 print(guess_password(password,extended))
```

Task 1 - part 5

Run your program.

Follow the instructions below and note down the results.

Instruction	Number of attempts	Time taken (round up to two decimal places)
Run the program with the password 'abc'		
Change the password to 'Ab1'		
Change the password to 'Abc1?'		
Change the password to 'AB C 1'		

Task 1 - part 6

Thinking about the exercise that you just completed, what simple password rules would you set yourself to reduce the chance of a brute force attack being successful?

What rules do you think a company might place on their login system to reduce the chance of a brute force attack being successful?

The Computer Misuse Act (1990): Fact sheet

The Computer Misuse Act (1990) and its amendments were created so that unauthorised access to computers and crimes committed using a computer could be prosecuted. The act is based on three principles and makes the following actions illegal:

Law	Punishment
Unauthorised access to digital/computer material. This means a person asking a computer to perform any function with the intent of accessing anything on the computer for which they do not have permission, and for which they know they do not have permission.	Punishable by up to two years in prison and a £5,000 fine.
Unauthorised access to digital/computer material with intent to commit or facilitate the commission of further offences. This means a person gaining access to a computer without permission in order to commit another crime or to enable someone else to commit a crime.	Punishable by up to five years in prison and an unlimited fine determined by the damage caused and the severity of the crime.
Unauthorised acts with intent to impair, or with recklessness as to impairing, the operation of a computer. This means a person intentionally impairing the operation of any computer or program, or intentionally preventing access to any data or program on any computer. This includes creating or supplying materials that could be used to carry out this offence.	Punishable by a prison sentence of up to ten years and an unlimited fine, but if the act puts life at risk or endangers national security, the sentence may be extended to life imprisonment.

Task 2: The 2016 Dyn Cyberattack

The Dyn cyberattack was a DDoS attack.

Answer the following three questions:

Which of the three sections of the Computer Misuse Act (1990) does a DDoS attack violate?	
Why do you think this?	
What is the maximum punishment for this crime under this act?	

Task 3: The Computer Misuse Act (1990)

Use the Computer Misuse Act fact sheet to help you determine whether or not the actions below would be prosecuted under the Computer Misuse Act (1990). Justify your answers.

Action	Does this break the Computer Misuse Act (yes/ no)?	If yes, which section does it break (1, 2, or 3)?	Justify your answer
Without permission, you took your friend's phone, correctly guessed their PIN, opened their banking app, and transferred money into your account.			
You used a brute force attack to gain access to your friend's email account to prove a point that their password isn't secure.			
A work colleague leaves their computer unlocked when away from their desk, and you go onto their computer and read their emails.			
You used a tool you downloaded to knock a friend offline from an online game they were beating you at.			