Task A

1. What is a brute force attack?

|  |
| --- |
| A brute force attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page. Hackers work through all possible combinations hoping to guess correctly. |

1. Why do hackers use a brute force attack?

|  |
| --- |
| * Profiting from ads or collecting activity data * Stealing personal data and valuables * Spreading malware to cause disruptions * Hijacking your system for malicious activity * Ruining a website’s reputation |

1. What measures can users put in place to protect themselves from a brute force attack?

|  |
| --- |
| * Use an advanced username and strong password. * Remove any unused accounts with high-level permissions. * Limit the number of attempts to login/lock account after a number of unsuccessful attempts. * Use of CAPTCHA for repeated login attempts. * Use of encryption. * Use two-factor authentication. |

1. Below is an article about a brute force attack on the Scottish Parliament.



What actions were performed by the hackers during this attack?

|  |
| --- |
| Hackers had repeatedly tried to break past authentication screens to internal accounts by entering random passwords, although there has been no evidence that the attack succeeded. |

How did this impact MP’s?

|  |
| --- |
| Many MP’s had been locked out of their accounts and the main reason behind this was the use of weak passwords. |