# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The protocol used in this incident was the TCP 3-way handshake. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Initially things seem to be going well, the DNS responds correctly to the browser’s request and the browser initiates an HTTP request for the webpage to access the site. The compromised browser then initiates the download of malware to the browser and immediately requests a different DNS resolution to redirect the browser to. The browser was compromised using a brute force attack, which the threat actor was easily able to guess using the default admin password. Additionally, there were no controls in place to prevent a brute force attack. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| A quick and simple remediation for brute force attacks is to set a strong password policy. This may include an 8 character minimum, including capital letters, a number and/or a symbol to ensure that the time taken to brute force the password is not a viable option for threat actors. |