# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The network protocols identified are in the application layer of the TCP/IP model; DNS and HTTP. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| The incident started with multiple complaints from the customers to the helpdesk, stating about a change in the behavior of the website after forcing them to download a suspicious file. After that, the browser changed to another URL, where the contents are similar to the original one, but free.  To address the incident, a sandbox was created to reproduce it in a isolated environment. According to the source code and the logs obtained by capturing the traffic with a network protocol analyzer:   * Right after opening yummyrecipesforme.com, the website executes a javascript snippet that prompts the visitor to download a file. * After executing the file, the computer starts to run slower, and the browser is redirected to greatrecipesforme.com, where the contents of the original website are offered for free.   The website was compromised, so the incident was escalated to the web owner who reported that his credentials have been modified. This incident is now communicated to the web hosting provider.  The malicious actor was able to get the credentials of the administrator, so this incident is a brute force attack. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| To remediate further brute force attacks, I recommend improving password policies:   * Change default passwords to stronger and more complex passwords. * Limit the number of login attempts.   Other measures:   * Monitor login attempts. * Force the use of multi-factor authentication (MFA) |