# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The port 80 is used, to the protocol used here is HTTP.  Since the problem was in accessing the website, we know that HTTP is used.  We ran tcpdump, and showed us a lot of used of port 80. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Customers contacted the website’s helpdesk stating that they were requested to download a file upon opening the website, containing new recipes. Their computers were slowed down after this. The website owner tried logging in their account, but the password was changed.  The cybersecurity analyst used a sandbox environment to open the website, so it would not involve any risks. Then, the analyst ran tcpdump to  capture the network traffic packets produced by interacting with the website.  The analyst was prompted to download the file, accepted the download and ran it. The browser then redirected the analyst to a fake website (greatrecipesforme.com).  The cybersecurity analyst inspected the tcpdump log and observed that the  browser initially requested the IP address for the yummyrecipesforme.com  website. Once the connection with the website was established over the HTTP  protocol, the analyst recalled downloading and executing the file. The logs  showed a sudden change in network traffic as the browser requested a new IP  address for the greatrecipesforme.com URL. The user was forwarded to the greatrecipesforme.com website.  The senior cybersecurity professional discovered that an attacker had manipulated the website to add code and change the admin password. The team believes that the attacker used a brute force method to gain access. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| One security measure to implement should be better password regulations. For example, disallowing the use of old passwords. Having a set of requirements for the password( eg. 8 characters, 1 number and 1 special character, at least). To better prevent this, two-factor authentification(2FA) should be implemented. This could mean, confirming the identity using a one-time password(OTP), send through email/phone or similar methods.  This would strengthen the security and will make it less likely for a brute force attack to happen. |