Security incident report

Section 1: Identify the network protocol involved in the incident

The network protocol involved in this incident is HTTP, as evidenced by the log captured by a tcpdump

Section 2: Document the incident

In response to the incident, the analyst created a sandbox environment to avoid damage to company assets. When the website loads, they're prompted to download an executable file under the false pretense of a browser update.

Upon downloading the file, the browser then redirects them to another page with the URL "greatrecipesforme.com", which appears to mimic the original page, but offers the company's content for free.

Meanwhile on the log, the browser initially requests for the right address, only after downloading and executing the file that the browser goes to the fake website.

The team confirmed that the web server was impacted by a brute force attack. The malicious actor managed to guess the password. Also, there weren't any controls in place to prevent this type of attack.

Section 3: Recommend one remediation for brute force attacks

The team intends to implement Two Factor Authentication(2FA) in order to prevent brute force attacks.