Security incident report

Section 1: Identify the network protocol involved in the incident

DNS (Domain Name System): This is the protocol used to turn website names, like yummyrecipesforme.com, into IP addresses that computers use to access the site. It was also used when the browser was redirected to the fake website, greatrecipesforme.com.

Section 2: Document the incident

What Happened Initially:

- The website was attacked by someone who kept trying different default passwords until they got the right one.
- This allowed them to get into the website's control area (admin panel).

What the Attacker Did:

- They put a special JavaScript code on the website.
- This code made visitors download a file, pretending it was a browser update.

The Effects:

- Running the file sent users to a fake version of the website.
- Customers noticed their computers became slow and the website address changed.
- The website owner couldn't log into the admin panel anymore.

Looking Into It:

- We set up a safe testing area (sandbox) and watched what happened using a tool called tcpdump.
- We saw how the website connected to the internet, how the harmful file was downloaded, and the switch to the fake website.
- We confirmed that the JavaScript code was causing these issues.

Section 3: Recommend one remediation for brute force attacks

Setup Account Locks and Two-Step Verification:

- Limit how often someone can try to log in and we should make it so accounts get locked if someone enters the wrong password too many times. This stops continuous guessing.
- Adding two-step verification means even if someone guesses the password, they need another code (like one sent to a phone) to get in.
- Change passwords often and make them hard to guess.

- Watch for strange login attempts and be ready to act.