Security incident report

Section 1: Identify the network protocol involved in the incident

The log entry with the code **HTTP: GET / HTTP/1.1** shows the browser is requesting data from **yummyrecipesforme.com** with the **HTTP: GET** method using **HTTP** protocol version **1.1**. This could be the download request for the malicious file.

Section 2: Document the incident

The traffic is routed from the source computer to the DNS server again using port **.52444** to make another DNS resolution request. The DNS server routes the traffic to a new IP address (**192.0.2.172)** and its associated URL (**greatrecipesforme.com.http**). The traffic changes to a route between the source computer and the spoofed website (outgoing traffic: **IP your.machine.56378 > greatrecipesforme.com.http** and incoming traffic: **greatrecipesforme.com.http > IP your.machine.56378**). The port number (**.56378**) on the source computer has changed again when redirected to a new website.

Section 3: Recommend one remediation for brute force attacks

Some common measures organizations use to prevent brute force attacks and similar attacks from occurring include:

1. **Salting and hashing**
2. **Multi-factor authentication (MFA) and two-factor authentication (2FA)**
3. **CAPTCHA and reCAPTCHA**
4. **Password policies**