Security incident report

Section 1: Identify the network protocol involved in the incident
The DNS Network protocol is involved in this incident. The DNS protocol sends the domain name and the web address to a DNS server that retrieves the IP address of the website you were trying to access, in this case, Yummy Recipes For Me. The IP address is included as a destination address for the data packets traveling to the Yummy Recipes For Me web server.

Section 2: Document the incident
At 1418 gmt today a security incident was reported.on the DNS & HTTP traffic log file shows the source computer (**your.machine.52444**) using port **52444** to send a DNS resolution request to the DNS server (**dns.google.domain**) for the destination URL (**yummyrecipesforme.com**). The cybersecurity analyst used a sandbox environment to test the website without impacting the company network. Then, the analyst ran tcpdump to capture the network and protocol traffic packets produced by interacting with the website. The analyst was prompted to download a file claiming it would update the user's browser, accepted the download and ran it. The browser then redirected the analyst to a fake website (greatrecipesforme.com) that looked identical to the original site (yummyrecipesforme.com). The next section shows the source computer sending a connection request (**Flags [S]**) from the source computer (**your.machine.36086**) using port **36086** directly to the destination (**yummyrecipesforme.com.http**). The **.http** suffix is the port number; **http** is commonly associated with port 80. The reply shows the destination acknowledging it received the connection request (**Flags [S.]**). The communication between the source and the intended destination continues for about 2 minutes, according to the timestamps between this block (**14:18**) and the next DNS resolution request (see below for the **14:20** timestamp). 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 resolution for the greatrecipesforme.com URL. The network traffic was then rerouted to the new IP address for the greatrecipesforme.com website.

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.
Then, a sudden change happens in the logs. The traffic is routed from the source computer to the DNS server again using port **.52444** (**your.machine.52444 > dns.google.domain**) to make another DNS resolution request. This time, 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**). Note that the port number (**.56378**) on the source computer has changed again when redirected to a new website.

This network attack appears to be an IP spoofing is a network attack performed when an attacker changes the source IP (Yummy Recipes For Me web server to Great Recipes for me) of a data packet to impersonate an authorized system and gain access to a network. The senior cybersecurity professional analyzed the source code for the websites and the downloaded file. The analyst discovered that an attacker had manipulated the website to add code that prompted the users to download a malicious file disguised as a browser update. Since the website owner stated that they had been locked out of their administrator account, the team believes the attacker used a brute force attack to access the account and change the admin password. The execution of the malicious file compromised the end users' computers.

The attacker executed a brute force attack to gain access to the web host. They repeatedly entered several known default passwords for the administrative account until they correctly guessed the right one. After they obtained the login credentials, they were able to access the admin panel and change the website's source code. They embedded a javascript function in the source code that prompted visitors to download and run a file upon visiting the website. After running the downloaded file, the customers are redirected to a fake version of the website where the seller's recipes are now available for free.

Section 3: Recommend one remediation for brute force attacks
IT support recommends the following actions to prevent brute force attacks using a combination of authentication measures. Implementing various OS hardening tasks can help prevent brute force attacks. Our analysis concludes the attacker used a brute force attack to gain access and compromise a network. IT support recommends with immediate effect that we establish a policy to immediately change default. Passwords are required to be 12 characters long, and must include lowercase, uppercase, a minimum of two numbers and two special characters i.e. *!@#$%&.