Explained: Security Incident Report

Section 1: Identify the network protocol involved in the incident
Hypertext transfer protocol (HTTP) is the protocol that was impacted by the incident. The information required to draw this conclusion came from running tcpdump, visiting the yummyrecipesforme.com website, and identifying the issue. These actions allowed us to record protocol and traffic activity in a DNS & HTTP traffic log file. At the application layer, the malicious file is seen being transferred to the users' computers over the HTTP protocol.

This activity's main objective was to determine the network protocol that was utilized during the incident. The report's opening sentence discloses the resolution to that action. The scenario's data, the DNS & HTTP log, and your knowledge of the TCP/IP model from this course were used to determine the protocol involved.:

- The DNS & HTTP log reveals that a request to the DNS server is made to find the IP address associated with the URL yummyrecipesforme.com. The appropriate IP address is returned by the DNS server. This is how the browser directs users to the appropriate website.
- According to the situation, a feature on the website asks users to download a file to upgrade their browsers as soon as the website loads. The scenario and the logs both show that this activity takes place via the HTTP protocol, which, as you already know, is a component of the TCP/IP model's application layer. For a description of the evidence found in the log, please read the article "How to read the DNS & HTTP traffic log" referenced in Step 2 of the activity.
- The logs indicate that following the user's download and execution of the file, the user's browser makes a fresh call to the DNS server to determine the IP address for a different URL: greatrecipesforme.com. Users are forwarded to this new website through HTTP after the DNS server resolves the URL.

Section 2: Document the incident
Numerous users complained to the website's owner that they had to download and run a file in order to update their browsers after visiting the page. Since then, their personal computers have been running sluggish. When the owner of the website attempted to enter into the web server, they discovered their account had been locked out. The website was tested in a sandbox environment by the cybersecurity expert without affecting the corporate network. To record the network and protocol traffic packets generated by interacting with the website, the analyst then used tcpdump. The analyst agreed to the request to download a file that would allegedly update the user's browser and then execute it. The analyst was then sent by the browser to a false website (greatrecipesforme.com) that had the exact same design as the real website (yummyrecipesforme.com). The security expert looked through the tcpdump record and noticed that the browser had asked for the yummyrecipesforme.com website's IP address at first. The analyst remembered downloading and running the file after the HTTP protocol connection with the website was made. The network traffic patterns in the logs abruptly changed as the browser asked for a new IP address to resolve the greatrecipesforme.com URL. The network traffic was then diverted to the greatrecipesforme.com website's new IP address. The senior cybersecurity expert examined the downloaded file and the website's source code. The analyst found that a hacker had added code to the website by manipulating it, prompting users to download a malicious file that was passed off as a browser update. The team thinks the attacker performed a brute force assault to access the account and modify the admin password because the website owner claimed they had been locked out of their administrator account. The PCs of the end users were infected when the malicious file was executed.

Your analysis of the log file and the activity's Scenario section should be included in Section 2 of the report. To better explain the inquiry and analysis process, you ought to have made connections between these events and what you have learned in the course. Note that even though you are the cybersecurity analyst outlining actions you took, it is standard report writing practice to refer to all parties involved in the third person (e.g., "the cybersecurity analyst" or "they").

1. The events and issues mentioned when the incident was originally reported are summarized in the first paragraph. The scenario's opening paragraph contains this information.
2. The testing procedures used to investigate this incident are described in the second paragraph. The scenario section also includes this information. You ought to have provided a written summary of these actions.
3. The analytical process is described in the third paragraph. The scenario and the log file both contain this information. In Step 2 of the activity, you can access the article "How to read the DNS & HTTP traffic log" to assist you in analyzing the log file.
4. The senior cybersecurity analyst's findings and those of the incident management team about the attack's underlying causes are added in the final paragraph.

Section 3: Recommend one remediation for brute force attacks
Two-factor authentication (2FA) is one security solution the team intends to use to defend against brute-force attacks. Users will also be required to confirm a one-time password (OTP) issued to either their email address or phone number as part of this 2FA strategy in order to verify their identity. The user will have access to the system once they have verified their identity using their login information and the OTP. A brute force attack by a bad actor is unlikely to succeed since the system needs extra authorization.

You were required to address brute force assaults in the third section. You were supposed to choose one of the choices in the reading regarding brute force attacks. The remediation approach and its operation should then have been described in your own words.