Security Incident Report

Section 1: Identify the network protocol involved in the incident

The network protocols involved in this incident were **DNS (Domain Name System)** and **HTTP (Hypertext Transfer Protocol)**.

DNS was used by the browser to resolve the domain names yummyrecipesforme.com and greatrecipesforme.com into their corresponding IP addresses. After the IP addresses were obtained, HTTP was used to request and load the web pages from those servers. HTTP was also used to deliver the malicious JavaScript code and initiate the download of the executable malware file.

Section 2: Document the incident

This security incident occurred when visitors attempted to access the website **yummyrecipesforme.com**. A former employee performed a brute force attack on the administrative account by repeatedly guessing default passwords until access was gained. Once authenticated, the attacker modified the website's source code and embedded malicious JavaScript.

When users visited the website, the malicious script prompted them to download and execute a file. After execution, users were redirected from yummyrecipesforme.com to greatrecipesforme.com, a malicious website hosting malware. Customers reported system slowdowns and unexpected website redirection.

Tcpdump logs showed DNS requests and responses followed by HTTP requests to both the legitimate and malicious websites. The website owner was locked out of the admin panel after the attacker changed the password. The incident resulted in malware distribution, loss of administrative access, and damage to customer trust.

Section 3: Recommend one remediation for brute force attacks

To prevent brute force attacks in the future, the organization should **implement account lockout controls**. This security measure would automatically lock administrative accounts after a predefined number of failed login attempts, preventing attackers from continuously guessing passwords. Combined with strong password policies, this control would significantly reduce the risk of unauthorized access.

Activity Exemplar: Apply OS hardening techniques

Section 1: Identify the network protocol involved in the incident
The protocol involved in the incident is the Hypertext transfer protocol (HTTP). Since the issue was with accessing the web server for yummyrecipesforme.com, we know that requests to web servers for web pages involve http traffic. Also, when we ran tcpdump and accessed the yummyrecipesforme.com website the corresponding tcpdump log file showed the usage of the http protocol when contacting the . The malicious file is observed being transported to the users' computers using the HTTP protocol at the application layer.

Section 2: Document the incident
Several customers contacted the website's helpdesk stating that when they visited the website, they were prompted to download and run a file that contained access to new recipes. Their personal computers have been operating slowly ever since. The website owner tried logging into the web server but noticed they were locked out of their account. The cybersecurity analyst used a sandbox environment to open the website without impacting the company network. Then, the analyst ran tcpdump to capture the network traffic packets produced by interacting with the website. The analyst was prompted to download a file claiming it would provide access to free recipes, accepted the download and ran it. The browser then redirected the analyst to a fake website (greatrecipesforme.com). 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 address for the greatrecipesforme.com URL. The network traffic was then rerouted to the new IP address for the greatrecipesforme.com website. 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.

Section 3: Recommend one or more remediations for brute force attacks
One security measure the team plans to implement to protect against brute force attacks is to disallow previous passwords from being used. Since the vulnerability that lead to this attack was the attacker's ability to use a default password to log in, it's important that we prevent any old passwords such as default passwords from being used to reset the password. Another supportive measure is to require more frequent password updates, so in case any unauthorized person becomes aware of the password, they are less likely to be able to use that password if the password is updated sooner than later. Finally, another helpful solution is to implement two-factor authentication (2FA). 2FA requires authentication via a password and also by confirming a one-time passcode (OTP) sent to either their email or phone. Once the user confirms their identity through their login credentials and the OTP, they will gain access to the system. Any malicious actor that attempts a brute force attack will not likely gain access to the system because it requires additional authentication.

The primary goal of this activity was to identify the network protocol used in the incident. The first line of the report announces the answer to that step. The protocol involved was determined by using information presented in the scenario, the DNS & HTTP log, and the knowledge you have learned about the TCP/IP model in this course:

- The tcpdump log shows a request is sent to the DNS server to resolve the IP address for the yummyrecipesforme.com URL. The DNS server replies with the correct IP address. The browser uses this to direct users to the correct website.
- The scenario states that when the website loads, a function on the website prompts users to download a file to access free recipes. Both the scenario and the logs indicate this activity occurs over the HTTP protocol, which you previously learned is part of the application layer of the TCP/IP model. Please review the article "How to read the tcpdump traffic log" linked in Step 2 of the activity for an explanation of the evidence found in the log.
- After the user downloads and runs the file, the logs show that the user's browser sends a new request to the DNS server to retrieve the IP address for a different URL:

greatrecipesforme.com. The DNS server sends the IP address to the users' browser and the users are redirected to this new website over HTTP.

Section 2 of the report should contain your interpretation of the log file and the Scenario section in the activity. You should have connected these events to what you have learned in the course to help you describe the investigation and analysis process. Note that it is a common practice for report writing to refer to all people involved in the third person (e.g., "the cybersecurity analyst" or "they"), even when you are the cybersecurity analyst describing actions you performed.

1. The first paragraph summarizes the events and problems identified when the incident was first reported. This information can be found at the beginning of the scenario.

2. The second paragraph describes the testing activities involved in investigating this event. This information is also provided in the scenario section. You should have summarized these activities in your own words.

3. The third paragraph describes the analysis work. This information is available in the scenario and the log file. The article "How to read the tcpdump traffic log" is available in Step 2 of the activity to help you interpret the log file.

4. The final paragraph adds what the senior cybersecurity analyst and the incident management team concluded about the root cause of the attack.

In the third section, you were to write about addressing brute force attacks. You should have selected at least one or more of the options provided in the reading about brute force attacks. Then you should have explained the remediation method and how it works in your own words.