# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| Application layer: the dns server has been redirected to other url | |
|

| **Section 2: Document the incident** |
| --- |
| When someone visit the website the yummyrecipesforme.com someone embedded a javascript that will download a file and making it redirected to other website to make the content for free |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| The owner should add a mfa. |

## **Step 3: Identify the network protocol involved in the incident**

**Network layer : using devices and computer sandbox**

**Internet layer: the device requesting for connection to yummyrecipesforme.com**

**Transport layer: when the transporting of data packets someone was meddling in the middle and making it replay in after 2 or 5mins and changing its port**

**Application layer: the dns server has been embedded a javascript that download a file to redirect to other website**

## **Step 4: Document the incident**

## **Summarize the incident in the second section of the report. Provide as many details and facts as possible in your documentation. When writing the documentation, be sure to:**

## **Avoid using strong emotional language (good, terrible, awful, etc.).**

## **Include as many facts about the issue as you can, including where the incident occurred, how it happened, whether anyone witnessed it, how it was discovered, etc.**

## **Indicate your sources for information and evidence.**

## **The disgruntled baker execute a brute for in yummyrecipesforme.com and able to guess the password, he embedded a javascript to make the url download a malicious file when visitors visit the website it redirects to a spoof website where they can see the selling books for free. As shown in tcpdump it change ip address and port was in full so the website were been getting slow, to make it avoided the owner should make a mfa to make sure the security of the website he has.**

## **Step 5: Recommend one remediation for brute force attacks**

After documenting the incident, write one recommendation to help your organization prevent brute force attacks in the future.

Some of the common security methods used to prevent brute force attacks include:

* Requiring strong passwords
* Enforcing two-factor authentication (2FA)
* Monitoring login attempts
* Limiting the number of login attempts

Select one security measure, and explain why it is effective in section three of the security incident report template.

The more safety measures that are in place, the less likely a malicious actor will be able to access sensitive information.

Website should implement 2fa because this will make the website stronger and couldnt get bruteforce.

SOLUTION:

# Activity Exemplar: Apply OS hardening techniques

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The protocol impacted in the incident is Hypertext transfer protocol (HTTP). Running tcpdump and accessing the yummyrecipesforme.com website to detect the problem, capture protocol, and traffic activity in a DNS & HTTP traffic log file provided the evidence needed to come to this conclusion. 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 owner stating that when they visited the website, they were prompted to download and run a file that asked them to update their browsers. 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 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 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 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 remediation for brute force attacks** |
| --- |
| One security measure the team plans to implement to protect against brute force attacks is two-factor authentication (2FA). This 2FA plan will include an additional requirement for users to validate their identification by confirming a one-time password (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 authorization. |