## **Scenario**

# 

# Review the scenario below. Then complete the step-by-step instructions.

# You are a cybersecurity analyst for yummyrecipesforme.com, a website that sells recipes and cookbooks. A former employee has decided to lure users to a fake website with malware.

# The baker 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 embedding the malware, the baker changed the password to the administrative account. When customers download the file, they are redirected to a fake version of the website that contains the malware.

# Several hours after the attack, multiple customers emailed yummyrecipesforme’s helpdesk. They complained that the company’s website had prompted them to download a file to access free recipes. The customers claimed that, after running the file, the address of the website changed and their personal computers began running more slowly.

# In response to this incident, the website owner tries to log in to the admin panel but is unable to, so they reach out to the website hosting provider. You and other cybersecurity analysts are tasked with investigating this security event.

# To address the incident, you create a sandbox environment to observe the suspicious website behavior. You run the network protocol analyzer tcpdump, then type in the URL for the website, yummyrecipesforme.com. As soon as the website loads, you are prompted to download an executable file to update your browser. You accept the download and allow the file to run. You then observe that your browser redirects you to a different URL, greatrecipesforme.com, which contains the malware.

# The logs show the following process:

# The browser initiates a DNS request: It requests the IP address of the yummyrecipesforme.com URL from the DNS server.

# The DNS replies with the correct IP address.

# The browser initiates an HTTP request: It requests the yummyrecipesforme.com webpage using the IP address sent by the DNS server.

# The browser initiates the download of the malware.

# The browser initiates a DNS request for greatrecipesforme.com.

# The DNS server responds with the IP address for greatrecipesforme.com.

# The browser initiates an HTTP request to the IP address for greatrecipesforme.com.

# A senior analyst confirms that the website was compromised. The analyst checks the source code for the website. They notice that javascript code had been added to prompt website visitors to download an executable file. Analysis of the downloaded file found a script that redirects the visitors’ browsers from yummyrecipesforme.com to greatrecipesforme.com.

# The cybersecurity team reports that the web server was impacted by a brute force attack. The disgruntled baker was able to guess the password easily because the admin password was still set to the default password. Additionally, there were no controls in place to prevent a brute force attack.

# Your job is to document the incident in detail, including identifying the network protocols used to establish the connection between the user and the website. You should also recommend a security action to take to prevent brute force attacks in the future.

# 

# 

# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The network protocol involved was the http as there was an error connecting the server.Through observation of the log file it is more clear that the error is with http as http protocol was used to connect to the server. | |
|

| **Section 2: Document the incident** |
| --- |
| There were emails and complaints from the users saying that when they visit a website they are forced to download one application to get a discount on recipe books and after downloading that software the computer is showing abnormal behavior and becoming slow. Admin tried to login but he is unable to do so.It means that the admin credentials have been changed.  The security analyst used the sandbox to open the website without causing any harm to the organization's network.Analyst checked the website and ran tcpdump then a prompt appeared showing a software to download which will give access to free recipe books. Analyst downloaded the software and ran it. After running it the browser redirected the analyst to another fake website.  The senior professional inspected the source code for the website and the downloaded file. The analyst discovered that an attacker had added some javascript code that prompted the users to download a malicious file. 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** |
| --- |
| The attacker was able to access the administrator account because there was no password policy that would suggest changing passwords after a certain amount of time ; stronger password policies need to be implemented.  Password policy should be in such a way that it should not allow new passwords resembling old passwords in any way.  Even if sometime any threat actor is able to crack the administrative password, if there is Multi-Factor Authentication (MFA) then it would avoid entering the administrative login. |