

# Activity: Apply OS hardening techniques

You are a cybersecurity analyst for [yummyrecipesforme.com](https://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.com](https://yummyrecipesforme.com)'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](https://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](https://greatrecipesforme.com), which contains the malware.

The logs show the following process:

1. The browser initiates a DNS request: It requests the IP address of the [yummyrecipesforme.com](https://yummyrecipesforme.com) URL from the DNS server.
2. The DNS replies with the correct IP address.
3. The browser initiates an HTTP request: It requests the [yummyrecipesforme.com](https://yummyrecipesforme.com) webpage using the IP address sent by the DNS server.
4. The browser initiates the download of the malware.
5. The browser initiates a DNS request for [greatrecipesforme.com](https://greatrecipesforme.com).
6. The DNS server responds with the IP address for [greatrecipesforme.com](https://greatrecipesforme.com).
7. The browser initiates an HTTP request to the IP address for [greatrecipesforme.com](https://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](https://yummyrecipesforme.com) to [greatrecipesforme.com](https://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.

## **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 led 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.