# Activity Exemplar: Apply OS hardening techniques

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The primary protocol involved in this incident is the Hypertext Transfer Protocol (HTTP). Since users experienced issues accessing the website *yummyrecipesforme.com*, and web page requests typically use HTTP, this indicates that HTTP traffic is directly affected. Additionally, tcpdump logs confirmed that HTTP was used when accessing the site. The logs also show that a malicious file was delivered to users via the HTTP protocol at the application layer, further confirming HTTP’s role in the incident. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Several customers reported being prompted to download a file offering new recipes after visiting *yummyrecipesforme.com*. After running the file, their computers began performing slowly. The website owner also reported being locked out of their admin account.  A cybersecurity analyst used a sandbox to safely test the site and captured network traffic with tcpdump. After downloading and running the suspicious file, the browser redirected to *greatrecipesforme.com*. Logs showed a sudden switch in traffic to this new domain.  Further analysis revealed that the site was compromised with malicious code prompting users to download a fake browser update. The attacker likely used a brute-force attack to gain admin access and upload the malicious content. Running the file compromised user systems. |

|  |
| --- |
| **Section 3: Recommend one or more remediations for brute force attacks** |
| To protect against brute force attacks, the team plans to implement several security measures. First, users will be prevented from reusing previous or default passwords, which was the vulnerability exploited in the current incident. Additionally, password update requirements will be enforced more frequently to limit the opportunity for unauthorized access. Finally, two-factor authentication (2FA) will be introduced, requiring users to verify their identity using both a password and a one-time passcode (OTP) sent to their email or phone. This added layer of security makes brute force attacks significantly less effective. |