Case Summary from Notes

This is the case you're supposed to write about:

- **Initial Trigger:**

  Customers report being prompted to download a suspicious file from yummyrecipesforme.com. Their computers slow down after.
- **Investigation Actions:**
  - Cybersecurity team used tcpdump in a sandbox to inspect the site
  - The site used HTTP protocol to serve a malicious file
  - After the file was downloaded, traffic was redirected to greatrecipesforme.com
  - The web server owner is locked out of their admin account
- **Findings:**
  - The site was compromised and modified to inject malicious code
  - The attacker likely used a brute-force attack to gain admin access
  - The malicious file acts like a fake browser update
- **Remediation Options (from exemplar):**
  - Prevent reuse of old/default passwords
  - Enforce regular password changes
  - Implement 2FA

Security incident report

Section 1: Identify the network protocol involved in the incident

The incident involved the Hypertext Transfer Protocol (HTTP). This protocol was used to transmit a malicious file from the compromised website (yummyrecipiesforme.com) to users’ machines. Packet analysis from `tcpdump` confirmed HTTP traffic during the download process, which eventually redirected users to greatrecipiesforme.com.

Section 2: Document the incident

Multiple users reported that visiting the website yummieresipesforme.com triggered a prompt to download a file labeled as a recipe bundle. After downloading and executing the file, their computers experiences performance issues. The site owner attempted to access the admin panel but found their credentials no longer worked.

The cybersecurity team created a sandbox environment to safely interact with the website. Using tcpdump, the team captured packets showing an initial DNS resolution followed by an HTTP request to the original site. Shortly after the file was downloaded, traffic shifted to greatrecipesforme.com, a known spoof domain.

Source code analysis revealed that the original website had been injected with malicious code that prompted a fake update download. The admin account was likely accessed using a brute-force attack, which allowed the attacker to make unauthorized changes to the site’s content.

Section 3: Recommend one remediation for brute force attacks

To protect against future brute-force attacks, the team recommends:

- Implementing two factor authorization (2FA) on all administrator accounts
- Disabling the reuse of old or default passwords
- Enforcing regular password updates

These measures would limit the effectiveness of brute-force attempts and add a second layer of authentication, reducing the likelihood of unauthorized access.