Activity Overview

In this activity, you will take on the role of a cybersecurity analyst working for a company that hosts the cooking website, yummyrecipesforme.com. Visitors to the website experience a security issue when loading the main webpage. Your job is to investigate, identify, document, and recommend a solution to the security problem. When investigating the security event, you will review a tcpdump log. You will need to identify the network protocols used to establish the connection between the user and the website. Network protocols are the communication rules and standards networked devices use to transmit data. Unfortunately, malicious actors can also use network protocols to invade and attack private networks. Knowing how to identify the protocols commonly used in attacks will help you protect your organization's network against these types of security events.

To complete the assignment, you will also need to document what occurred during the security incident. Then, you will recommend one security measure to implement to prevent similar security problems in the future.

Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

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 former employee/ hacker 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 hacker 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:

1. The browser initiates a DNS request: It requests the IP address of the 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 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.
6. The DNS server responds with the IP address for greatrecipesforme.com.
7. 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 hacker 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
During the security incident on yummyrecipesforme.com, the following network protocols were observed:

- **DNS(Domain name system)**: Used to resolve the domain names (yummyrecipesforme.com and greatrecipesforme.com) to their respective Ip adresses.
- **HTTP(Hypertext Transfer protocol)**: Used to requestr and load the compromised webpage from yummy recpesforme.com and the malicous site greatrecipesforme.com.
- **TCP(Transmission Control Protocol)**: The transport layer protocol responsible for reliable communication between the user's browser and the webserver.

Section 2: Document the incident
Incident summary: A former emplyee executed a brute force attack(a cyberattack that uses trial and error to guess passwords, login credentials, or encryption keys.) on yummyrecipesforme.com to gain unauthorized acces to the admin panel. *The hacker used a list of known default passwords until sucessfuly logging in*, as the admin credentials were still ser to default.
Once inside, the hacker modified the website's source code by embedding a malicious Javascript function> this script prompted visitors to download an executable file under the pretense of a browser update. Upon execution, the malware redirected users to *greatrecipesforme.com*, **a fraudulent site designed to infect computers**.
Investigating Findings:

- Costumers reported being prompted to download a suspicious file.
- Website traffic logs and a tcpdump analysis confirmed:
  - A DNS request was made for yummyrecipesforme.com.
  - A legimate HTTP request was sent to the site.
  - The browser was instructed to download an unauthorized executable file.
  - A subsequent DNS request was made for *greatrecipesforme.com.*
  - The browser then redirected to greatrecipesforme.com, which hosted a malware.
- A senior cybersecurity analyst confirme the presence of a malicious Javasrcipt function in the website's source code.

Section 3: Security recomendations
To prevent similar attacks in the future, the following security measures should be implemented:

- **Enforce Strong Authentication Measures:**
  - Implementing ***MFA*** for all administrative accounts.
  - Enforce ***strong password policies*** requiring complex passwords.
  - ***Disable default credential*** on all administrative accounts.
- **Brute Force Attack Mitigation:**
  - Set up a**ccount lockout policies** after multiple failed login attempts.
  - Implent **rate limiting and CAPTCHA challenges** to slow down automated login attempts.
  - Monitor and analyze login attempts using **intrusion detection systems(IDS)**.
- **Additional Security Measures:**
  - Conduct re**gular security audits** to identify vulnerabilities.
  - Use Content Security Policy(CSP) to restrict JavaScript execution.
  - Ensure regular softwarew updates to patch known security flaws.