The Security incident report (YummyRecipesForMe.com)(My Responses)

Section 1: Identify the network protocol involved in the incident
Based on the scenario, the given supporting documents, and the events that happened, I hypothesize that the network protocol involved in this security incident is the Hypertext Transfer Protocol (HTTP). The given documents explains that HTTP is used to request and deliver web pages and content between users and web servers. In this case, I noticed that it was used during both the initial interaction with the legitimate website (yummyrecipesforme.com) and the redirection to the malicious website (greatrecipesforme.com). This foreshadows and tells me that the incident started when a former employee hacked into the company's website which then the hacker gained unauthorized access to the web host by using a brute force attack, involving guessing the passwords (social engineering techniques) until the correct one was found. Then with the other notes, it allowed me to see that once inside the administrative panel, the hacker modified the website's source code by inserting a JavaScript code that prompted visitors to download a malicious executable file, containing to offer free recipes but actually contained malware codes (computer programming scripts/codes). Then, the cybersecurity team used a sandbox environment to safely analyze the attack using a network protocol analyzer called tcpdump to capture the network traffic while visiting the infected website. Based on the sequence of events, I can see how when the analyst accessed yummyrecipesforme.com, the browser sent a DNS request to resolve the IP address for the site. Then, the DNS server replied with the correct IP address, and the browser initiated an HTTP request to load the page. Also, with the supporting documents given, this tells me that after, the browser prompted the analyst to download a file claiming to be a browser update. I can see how the analyst downloaded and ran the file where the browser redirected to a different website c called greatrecipesforme.com which is a new URL accessed over HTTP; confirmed by the tcpdump logs that both websites were using HTTP (which operates at the application layer of the TCP/IP model based on the notes, evidences, and documents provided). To get to the point, the virus/malware file was delivered/sent to users over HTTP, making this protocol a part of how the attack was executed and became the cybersecurity incident (social engineering techniques and attacks).

Section 2: Document the incident
As explained of the whole scenario and what happened previous, basically, multiple customers contacted the helpdesk for yummyrecipesforme.com and reported that the website had prompted them to download a file in order to access new recipes. After clicking and running the file from that website, the website address changed and their personal computers started to slow down and when the website owner attempted to log in to the administrative panel to investigate the issue, the owner was locked out. As a result, the web owner contacted the hosting provider for help and then the cybersecurity team, including the analyst, was asked to investigate the situation. Based on the evidences provided and the sequences of events; the analyst used a sandbox environment to avoid affecting the main network, running a tcpdump to monitor network traffic and then accessed the website, and investigate the issue safely. Then, when the analysist, visited yummyrecipesforme.com, the browser immediately prompted a download of a clickable file stating an excuse that this was because it needed to update the browser, and allowed the file to run. By allow the file to run, the browser redirected to a different website: greatrecipesforme.com where the tcpdump logs confirmed the pattern of the virus/malware form the clickable file downloaded. This was demonstrated based on the scenario and evidences where first, the browser made a DNS request for yummyrecipesforme.com, received the correct IP address, and loaded the website using HTTP. After downloading and running the executable, the browser made a new DNS request for greatrecipesforme.com. The DNS server returned an IP address for the new domain, and the browser connected to it via HTTP. This log confirmed that the file triggered a redirection to a fake site that delivered malware/virus. Because of this the analysist examined the code for what caused the DNS request and the IP exchange and found the that the JavaScript code embedded to it that prompted visitors to download the executable file, which is a script that redirected users to greatrecipesforme.com after execution. The analyst then realized that after this was already executed, it meant that the hacker accessed the admin account by using a brute force attack. And then the admin account still used the default password, and there were no security measures in place to block or detect repeated login attempts. Because of this, the analysist relied that once the hacker gained access, the hacker changed the admin password to prevent the site owner from regaining control. This obviously ends the investigation and concludes that the malicious code and executable file, users' computers were exposed to malware compromising the security and systems by damaging the credibility of the company’s website.

Section 3: Recommend one remediation for brute force attacks
Based on the scenario, supporting documents given, and the investigation these are my three recommendations: **1)** the system should be configured to prevent the use of default or previously used passwords as the attacker was able to log in using a default password, requiring strong, unique passwords is essential to implement good security hardening techniques. By doing these changes, it reduces the chances of an attacker guessing (brute force) or reusing old credentials (social engineering techniques); **2)** I recommended implementing two-factor authentication (2FA). With 2FA, because even if someone guesses the correct password, the person would also need to verify their identity using a second method like a one-time passcode (OTP) sent to a verified email or phone number, making it much harder for attackers to gain access, even with valid login credentials; **3)** I recommend that the company enforce stronger password updates or policies by requiring users to update their passwords regularly and implement strong password polices, which can reduce the window of opportunity for any leaked or guessed credentials to be used successfully.

Additional Information:

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.

The following supporting materials will help you complete this activity. Keep them open as you proceed to the next steps.

To use the supporting materials for this course item, click the link below and select *Use Template*.

Links to supporting materials:

- tcpdump traffic log

□ □ How to read the tcpdump log

Step 3: Identify the network protocol involved in the incident

As one of the cybersecurity analysts in this scenario, you are tasked with writing an incident report for this security event. Using the tcpdump log file, determine which network protocol is identified in the packet captures during the investigation. You will use what you learned about the four layers of the TCP/IP model and which protocols happen at each layer. If needed, you can review the video

and reading about the TCP/IP model

to use as guides for your response. Then review the tcpdump traffic log and record which protocol you identified in the first section of the security incident report template.

Step 4: Document the incident

Summarize the incident in the second section of the report. Provide as many details and facts as possible in your documentation. When writing the documentation, be sure to:

- Avoid using strong emotional language (good, terrible, awful, etc.).
- Include as many facts about the issue as you can, including where the incident occurred, how it happened, whether anyone witnessed it, how it was discovered, etc.
- Indicate your sources for information and evidence.

Writing accurate and detailed documentation for cybersecurity incidents can serve as a reference point for other cybersecurity analysts. Additionally, quality documentation can be used to educate other employees about cybersecurity measures taken within the company when incidents occur and can help businesses comply with various security audits.

Step 5: Recommend one remediation for brute force attacks

After documenting the incident, write one recommendation to help your organization prevent brute force attacks in the future.

Some of the common security methods used to prevent brute force attacks include:

- Requiring strong passwords
- Enforcing two-factor authentication (2FA)
- Monitoring login attempts
- Requiring more frequent password changes
- Disallowing previous passwords from being used
- Limiting the number of login attempts

Select one security measure, and explain why it is effective in section three of the security incident report template.

The more safety measures that are in place, the less likely a malicious actor will be able to access sensitive information.

Be sure to address the following criteria in your completed activity:

- Name one network protocol identified during the investigation
- Document the incident
- Recommend one security measure