To pass this course item, you must receive 100%, or 1 out of 1 point, by completing the following activity. You can learn more about graded and practice items in the course overview.

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 disgruntled baker has decided to publish the website's best-selling recipes for the public to access for free.

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 running the downloaded file, the customers are redirected to a fake version of the website where the seller's recipes are now available for free.

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 update their browsers. 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 is designed to look like the original site. However, the recipes your company sells are now posted for free on the new website.

The logs show the following process:

1. The browser requests a DNS resolution of the yummyrecipesforme.com URL.
2. The DNS replies with the correct IP address.
3. The browser initiates an HTTP request for the webpage.
4. The browser initiates the download of the malware.
5. The browser requests another DNS resolution for greatrecipesforme.com.
6. The DNS server responds with the new IP address.
7. The browser initiates an HTTP request to the new IP address.

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 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.

Step-By-Step Instructions

Follow the instructions and answer the question below to complete the activity. Then, go to the next course item to compare your work to a completed exemplar.

Step 1: Access the template

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

Link to template:

- Security incident report template

OR

If you don't have a Google account, you can download the template directly from the attachment below.

Security incident report template
DOCX File

Step 2

Step 2: Access supporting materials

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:

- DNS & HTTP traffic log
- How to read the DNS & HTTP log

OR

If you don't have a Google account, you can download the supporting materials directly from the attachment below.

DNS & HTTP traffic log
DOCX File

How to read the DNS & HTTP traffic log
DOCX File

Steps 3, 4, and 5

Step 3: Identify the network protocol involved in the incident

Imagine that you are one of the cybersecurity analysts in this scenario and you are tasked with writing an incident report for this security event. Using the DNS & HTTP log file you produced with tcpdump, 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 DNS & HTTP 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
- 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.

Pro tip: Save the template

Finally, be sure to save a blank copy of the template you used to complete this activity. You can use it for further practice or in your professional projects. These templates will help you work through your thought processes and demonstrate your experience to potential employers.

What to Include in Your Response

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