**Activity: Apply OS hardening techniques**

In this activity, you will take on the role of a cybersecurity analyst working for a company that hosts the cooking website yummyrecipesforme.com. Website visitors face a security issue when loading the main page. Their job is to investigate, identify, document, and recommend a solution to the security problem.

When investigating the security event, you'll 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 that networked devices use to transmit data. Unfortunately, malicious actors can also use network protocols to break into and attack private networks. Knowing how to identify the protocols commonly used in attacks will help you protect your organization's network from these types of security events.

To complete the task, you'll also need to document what occurred during the security incident. Next, you will recommend a security measure to implement to avoid similar security issues in the future.

Be sure to complete this activity before proceeding. The next course item will provide you with a complete copy to compare with your own work.

**Scenario**

You're a cybersecurity analyst at yummyrecipesforme.com, a website that sells recipes and cookbooks. A disgruntled baker decided to publish the site's best-selling recipes for the public to access for free.

The baker executed a brute force attack to gain access to the host. They repeatedly entered several known default passwords for the administrative account until they correctly guessed the correct password. After obtaining the login credentials, they were able to access the admin panel and change the source code of the website. They embedded a javascript function in the source code that asked visitors to download and run a file when visiting the site. After executing the downloaded file, 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, several customers sent emails to yummyrecipesforme's tech support. They complained that the company's website had asked them to download a file to update their browsers. Customers claimed that after running the file, the website address changed and their personal computers started to run more slowly.

In response to this incident, the website owner tries to log in to the admin panel but is unable to do so, so they contact the website's hosting provider. You and other cybersecurity analysts are tasked with investigating this security event.

To resolve the incident, you create a sandbox environment to observe suspicious website behavior. You run the tcpdump network protocol analyzer and type in the URL of the website, yummyrecipesforme.com. Once the website loads, you will be prompted to download an executable file to update your browser. You accept the download and allow the file to run. You then notice that your browser redirects you to a different URL, greatrecipesforme.com, which is designed to look like the original website. However, the recipes your business sells are now posted for free on the new website.

The logs show the following process:

1. The browser requests a DNS resolution from the URL yummyrecipesforme.com.
2. DNS responds with the correct IP address.
3. The browser initiates an HTTP request to the web page.
4. The browser starts downloading 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 site has been compromised. The analyst checks the source code of the website. They notice that javascript code has been added to prompt site visitors to download an executable file. Analysis of the downloaded file found a script that redirects visitors' browsers from yummyrecipesforme.com to greatrecipesforme.com.

The cybersecurity team reports that the web server has been impacted by a brute force attack. The disgruntled baker was able to guess the password easily because the admin password was still set as the default password. In addition, there were no controls to prevent a brute force attack.

Their 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 1: Access the template**

File "*Security incident report template*"

**Step 2: Access support materials**

"*DNS & HTTP traffic log" file*

File "How to read the DNS & HTTP traffic log"

**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 that security event. Using the DNS and HTTP log file produced with tcpdump, determine which network protocol is identified in the packet captures during the investigation. You'll use what you've learned about the four layers of the TCP/IP model and what protocols occur at each layer. If necessary, you can review the video and read about the TCP/IP model to use as a guide in your response. Next, review the DNS and 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 much detail and facts as possible in your documentation. When writing documentation, make sure to:

* Avoid using strong emotional language (good, terrible, horrible, etc.).
* Include as many facts about the issue as possible, including where the incident occurred, how it happened, whether anyone witnessed it, how it was discovered, etc.
* Indicate your sources of 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 the cybersecurity measures taken in the company when incidents occur and can help businesses comply with various security audits.

**Step 5: Recommend a solution for brute force attacks**

Once you've documented the incident, write a 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 a security measure and explain why it is effective in section three of the security incident report template.

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

**What to include in your answer**

Make sure you meet the following criteria in your completed activity:

* Cite a network protocol identified during the investigation
* Document the incident
* Recommend a safety measure

**Example Completed**

File "*Exemplary security incident report*"

Archive "*The Exemplar Explained - Security incident report exemplar*"

**Example Evaluation**

Compare the copy with your completed activity. Proofread your work using each of the criteria in the issue. What did you do well? Where can you improve? Use your answers to these questions to guide you as you progress through the course.

**Note**: The example represents a possible explanation for the problems that end users face. Yours will probably be different in some ways. The important thing is that you've identified the network protocols involved and created a report. In your role as a security analyst, you and your team would document any issues that occur on the network and come up with solutions to help prevent the same issues from occurring in the future. Good quality documentation can save time for you and your organization and potentially manage the attack from the start.

First, analyze the DNS and HTTP traffic log to identify a network protocol. Then, document the cybersecurity incident. Finally, recommend a security measure that your organization could implement to prevent brute force attacks in the future. Creating this process, in turn, will help improve the organization's security posture.

The copy is accompanied by the activity and presents an example of professional documentation that includes the following:

* A network protocol identified during the investigation
* Incident documentation
* A Recommended Security Measure