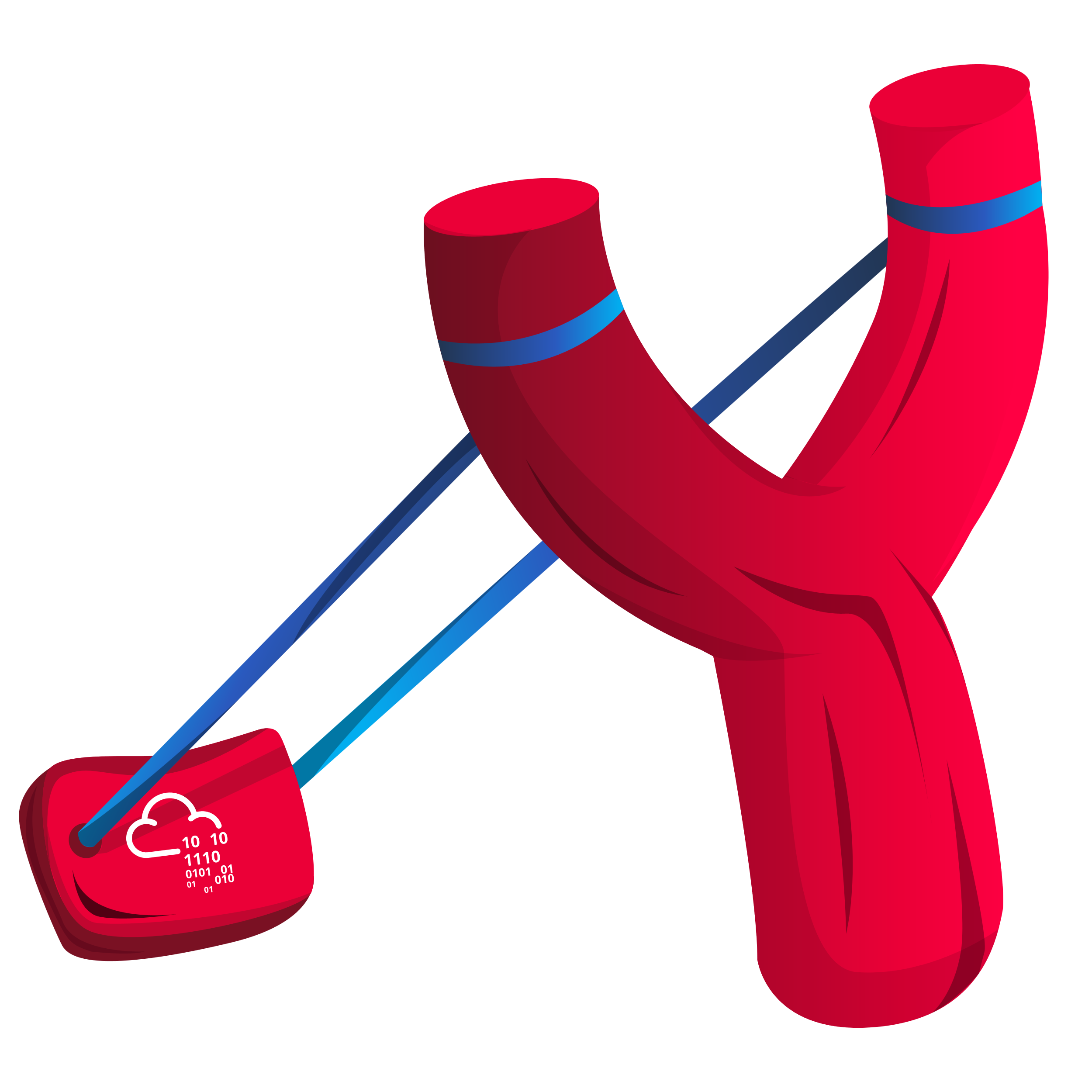
**Slingshot**



**Scenario**

Slingway Inc., a leading toy company, has recently noticed suspicious activity on its e-commerce web server and potential modifications to its database. To investigate the suspicious activity, they've hired you as a SOC Analyst to look into the web server logs and uncover any instances of malicious activity.

To aid in your investigation, you've received an Elastic Stack instance containing logs from the suspected attack. Below, you'll find credentials to access the Kibana dashboard. Slingway's IT staff mentioned that the suspicious activity started on **July 26, 2023**.

By investigating and answering the questions below, we can create a timeline of events to lead the incident response activity. This will also allow us to present concise and confident findings that answer questions such as:

* What vulnerabilities did the attacker exploit on the web server?
* What user accounts were compromised?
* What data was exfiltrated from the server?

Instructions

First, click **Start Machine** to start the VM attached to this task. You may access the VM using the AttackBox or your VPN connection. You can start the AttackBox by pressing the **Start AttackBox** button on the top-right of this room. **Note:** The Elastic Stack may take up to 5 minutes to fully start up. If you receive any errors, give it a few minutes and refresh the page.

Once online, navigate to http://MACHINE\_IP using a web browser.

You should see the Elastic login page. Please log in using the following credentials:

A screenshot of a computer

AI-generated content may be incorrect.

**Q1. What was the attacker's IP?**

Access Discover in Elastic and set the time range to **July 26, 2023**. Upon selecting transactions.remote\_address, an abnormal volume of traffic is observed, indicating the presence of the attacker's IP address.

A screenshot of a computer

AI-generated content may be incorrect.

*10.0.2.15Top of Form*

**Q2.**

**Bottom of Form**

**What was the first scanner that the attacker ran against the web server?**

Filtering for the attacker’s IP address and sorting the activities by date, starting with the oldest to find the first activities, we can see the scanner.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

*Nmap Scripting EngineTop of Form*

**Q3.**

**Bottom of Form**

**What was the User Agent of the directory enumeration tool that the attacker used on the web server?**

Directory enumeration uses brute force techniques, which can lead to a number of 404 and 200 status codes. By filtering out these 404 responses, the tool name was identified.

A screenshot of a computer

AI-generated content may be incorrect.

*Mozilla/5.0 (Gobuster)Top of Form*

**Q4.**

**Bottom of Form**

**In total, how many requested resources on the web server did the attacker fail to find?**

Since 404 errors have already been filtered out, the number of requests can be viewed directly on the same page.

A screenshot of a computer

AI-generated content may be incorrect.

*1867Top of Form*

**Q5.**

**Bottom of Form**

**What is the flag under the interesting directory the attacker found?**

Add Gobuster and the 200 response code to the filter. Searching for "flag" returns a single result containing the flag.

A screenshot of a computer

AI-generated content may be incorrect.

*a76637b62ea99acda12f5859313f539aTop of Form*

**Q6.**

**Bottom of Form**

**What login page did the attacker discover using the directory enumeration tool?**

Exclude 200 and 404 status codes to identify other responses. This revealed the login page.

A screenshot of a computer

AI-generated content may be incorrect.

*/admin-login.phpTop of Form*

**Q7.**

**Bottom of Form**

**What was the user agent of the brute-force tool that the attacker used on the admin panel?**

As login brute force attempts typically result in multiple 401 responses, we’ll exclude the 200 and 404 response codes, and focus on filtering with the 401 response code.

A screenshot of a computer

AI-generated content may be incorrect.

*Mozilla/4.0 (Hydra)Top of Form*

**Q8.**

**Bottom of Form**

**What username:password combination did the attacker use to gain access to the admin page?**

When access is obtained, the response code is not 401. Including this criteria in the filter gives only one result.

A screenshot of a computer

AI-generated content may be incorrect.

A base64 string is shown. This can be decoded using the base64 tool in CyberChef.

A screenshot of a computer

AI-generated content may be incorrect.

*admin:thx1138Top of Form*

**Q9.**

**Bottom of Form**

**What flag was included in the file that the attacker uploaded from the admin directory?**

Since an upload uses POST or PUT, not GET. Adding this to the filter, we get:

A screenshot of a computer

AI-generated content may be incorrect.

*THM{ecb012e53a58818cbd17a924769ec447}*

**Q10. Top of Form**

**Bottom of Form**

**What was the first command the attacker ran on the web shell?**

The filename for the uploaded file is ‘easy-simple-php-webshell.php’ and using the response code 200.

Sort the timestamp from oldest to newest to find the first command, which is in the http.url field.

A screenshot of a computer

AI-generated content may be incorrect.

*whoami*

**Q11. Top of Form**

**Bottom of Form**

**What file location on the web server did the attacker extract database credentials from using Local File Inclusion?**

While filtering **/admin/**, we detected path traversal requests.

A screenshot of a computer

AI-generated content may be incorrect.

*/etc/phpmyadmin/config-db.php*

Q12. Top of Form

Bottom of Form

What **directory** did the attacker use to access the database manager?

A close-up of a computer screen

AI-generated content may be incorrect.

*/phpmyadmin*

Q13. Top of Form

Bottom of Form

What was the name of the database that the attacker **exported**?

Using phpmyadmin\*export\* in the search query, we can see the exported database in the results with the http.url field.

A screenshot of a computer

AI-generated content may be incorrect.

*customer\_credit\_cards*

Q14. Top of Form

Bottom of Form

What flag does the attacker **insert** into the database?

The export was replaced with import in the phpmyadmin \*export\* search query. Upon examining the request body, a URL-encoded message is observed, as shown below:

"is\_js\_confirmed=0&db=customer\_credit\_cards&table=credit\_cards&token=302e562342217c5d6258344222294172&pos=0&goto=tbl\_sql.php&message\_to\_show=Your+SQL+query+has+been+executed+successfully.&prev\_sql\_query=INSERT+INTO+%60credit\_cards%60+(%60card\_number%60%2C+%60cardholder\_name%60%2C+%60expiration\_date%60%2C+%60cvv%60)+VALUES+('000'%2C+'c6aa3215a7d519eeb40a660f3b76e64c'%2C+'000'%2C+'000')%3B&sql\_query=INSERT+INTO+%60credit\_cards%60+(%60card\_number%60%2C+%60cardholder\_name%60%2C+%60expiration\_date%60%2C+%60cvv%60)+VALUES+('000'%2C+'c6aa3215a7d519eeb40a660f3b76e64c'%2C+'000'%2C+'000')%3B&sql\_delimiter=%3B&show\_query=1&fk\_checks=0&fk\_checks=1&SQL=Go&ajax\_request=true&ajax\_page\_request=true&\_nocache=169038208497548768&token=302e562342217c5d6258344222294172"

After URL decoding the message using Cyberchef, we get:

“is\_js\_confirmed=0&db=customer\_credit\_cards&table=credit\_cards&token=302e562342217c5d6258344222294172&pos=0&goto=tbl\_sql.php&message\_to\_show=Your SQL query has been executed successfully.&prev\_sql\_query=INSERT INTO `credit\_cards` (`card\_number`, `cardholder\_name`, `expiration\_date`, `cvv`) VALUES ('000', **'c6aa3215a7d519eeb40a660f3b76e64c'**, '000', '000');&sql\_query=INSERT INTO `credit\_cards` (`card\_number`, `cardholder\_name`, `expiration\_date`, `cvv`) VALUES ('000', 'c6aa3215a7d519eeb40a660f3b76e64c', '000', '000');&sql\_delimiter=;&show\_query=1&fk\_checks=0&fk\_checks=1&SQL=Go&ajax\_request=true&ajax\_page\_request=true&\_nocache=169038208497548768&token=302e562342217c5d6258344222294172"

Which is our flag

*c6aa3215a7d519eeb40a660f3b76e64c*

**Conclusion**

After completing the log investigation, you can present confident findings that an attacker compromised the web server and database. You managed to follow the timeline of events, allowing for a clearer understanding of the incident and actions performed.

In response to this incident, Slingway Inc. should address the identified vulnerabilities promptly to enhance the security of its web server. Furthermore, the company should take appropriate steps to notify affected customers about the data breach and implement proactive security measures to mitigate future attacks.

Your investigation's comprehensive findings and actionable insights will enable Slingway Inc. to mitigate the damage caused by the compromised server, bolster its cyber security posture, and safeguard its customers' trust. Well done!

*No answer needed*