

**INFORMES EJECUTIVO Y TÉCNICO**

**Resultados obtenidos para ser usuario con privilegios root explotando vulnerabilidades del sistema**

* Fecha: 24 de julio de 2024
* Cliente: Reto 7
* Consultora de Ciberseguridad: The Bridge - Accelerator
* Control de Cambios

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Versión | Documento | Fecha | Cambios | Autor | revisor | visto bueno |
| 1.1 | Informe de resultados | 03/07/2024 | Informe inicial | Victor Martínez | Ángel  Cardiel | Javier Tomás |

**Índice de Contenidos**

1. Introducción ----------------------------------------------------------------------------------3
2. Alcance ----------------------------------------------------------------------------------------3
3. Vulnerabilidades encontradas: ----------------------------------------------------------4
4. Dispositivo Metasploitable -------------------------------------------------------4
5. Dispositivo Winsploitable -------------------------------------------------------- 6
6. Recomendaciones generales: -----------------------------------------------------------9
7. Dispositivo Metasploitable -------------------------------------------------------9
8. Dispositivo Winsploitable ---------------------------------------------------------9
9. Conclusiones ---------------------------------------------------------------------------------9
10. Bibliografía ----------------------------------------------------------------------------------10
11. Dispositivo Metasploitable -----------------------------------------------------10
12. Dispositivo Winsploitable -------------------------------------------------------11

1. INTRODUCCIÓN

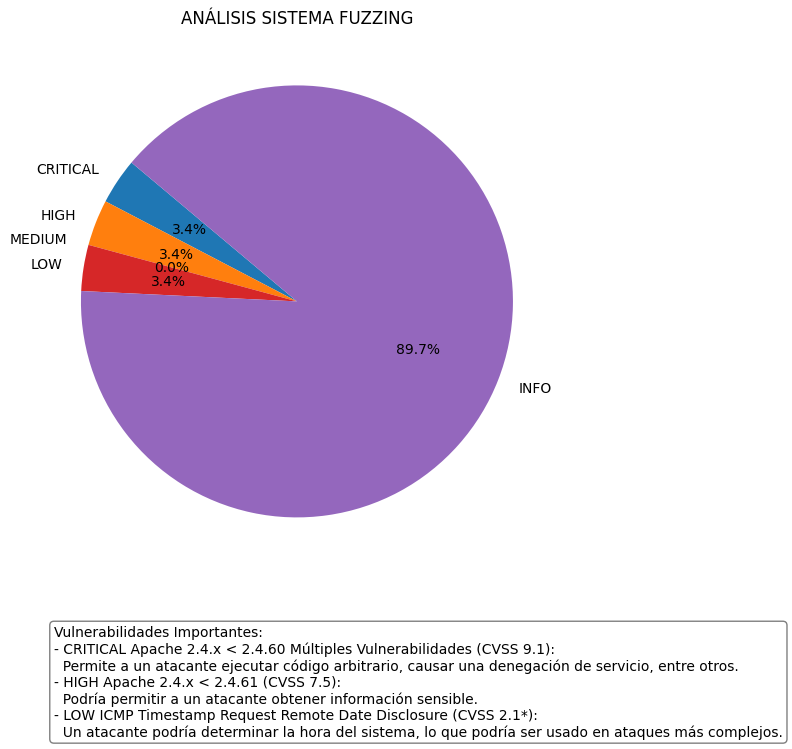
El presente informe está conformado por 2 partes: un informe ejecutivo, menos técnico y dirigido a informar a los latos cargos o ejecutivos de la compañía, y un informe técnico dirigido a los analistas de ciberseguridad y programadores que tengan que ejecutar las tareas para mitigar las vulnerabilidades explotadas, para mejorar los manuales de estrategia de la compañía para la detección, contención y respuesta ante incidentes críticos en su sistema.

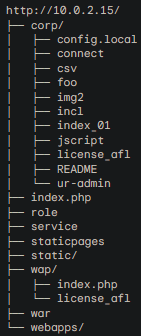
2. INFORME EJECUTIVO

1. Introducción. – Este informe tiene como objetivo presentar los resultados de las vulnerabilidades detectadas y explotadas en el equipo Fuzzing, de acuerdo con el contrato firmado entre ambas partes, en el que permiten la explotación del sistema con la finalidad de conseguir la autenticación por atacantes externos con usuarios con privilegios root. El equipo no tiene entorno grafico y apara acceder en línea de comandos hace falta una clave y contraseña que no aportan y se han usado para su explotación diversas herramientas de ciberseguridad, destacando alguna de ellas:

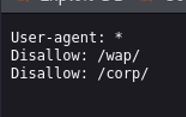
* Nessus Essentials. - Herramienta de escaneo de vulnerabilidades más populares y completas en el ámbito de la seguridad informática, que se utiliza para identificar vulnerabilidades en sistemas y redes, detectar configuraciones incorrectas y posibles puntos de entrada para ataques en una amplia gama de plataformas, clasificando estas en críticas, altas, medias e info.

En este ataque no ha sido necesario explotar ninguna de las vulnerabilidades detectadas, siendo las mas importantes, las que figuran al pie de la siguiente figura, donde se pueden observar los porcentajes de las vulnerabilidades encontradas, siendo los resultados muy buenos en general.



 Dirb**.** - Herramienta de seguridad y hacking web, comúnmente utilizada durante las fases de reconocimiento en pruebas de penetración, utilizándose para descubrir objetos y directorios ocultos o no listados en un servidor web, siendo muy útil para encontrar información sensible que ha sido mal configurada o expuesta por los administradores del sitio web.

Como se puede observar hay un directorio con amplia información del sistema, llamado *“Corp”,* donde se muestra la configuración local del sistema.

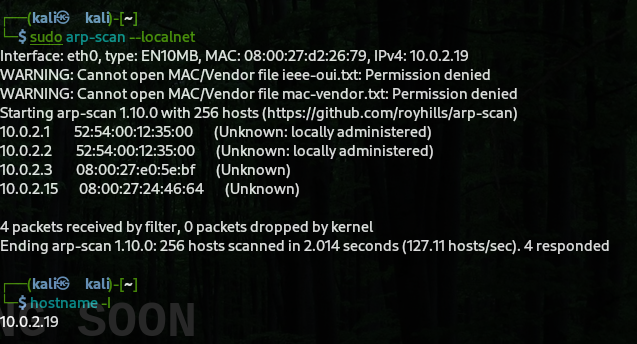
Desde el mismo navegador web, se puede acceder al archivo *“robots.txt*”, siendo éste usado por los administradores de sistemas para ocultar a la indexación ciertas carpetas que no desean que sean visibles,aportando pistas a los atacantes en que archivos indagar, pero como vemos aquí, le ha faltado ocultar aun mas su visibilidad.

Gobuster*. -* Herramienta de seguridad utilizada para realizar ataque por fuerza bruta de URLs (directorios y nombres de archivos) en servidores web y para la enumeración de subdominios, siendo ampliamente utilizada durante las fases de reconocimiento en pruebas de penetración y auditorías de seguridad.

Como se puede observar, al acceder al directorio *“corp”,* concretamente a su subdirectorio *“config.local”*, la carpeta “/users aparece en color verde, en la cual hay información de usuarios y claves del sistema.

1. Alcance. - El alcance se ha centrado en identificar y evaluar las debilidades de seguridad en el sistema, logrando, finalmente, la autenticación con un usuario con privilegios root, explotando algunas vulnerabilidades que pueden comprometer la integridad, confidencialidad y disponibilidad de los datos del mismo.
2. Vulnerabilidades explotadas. – Para conseguir el objetivo fijado en el contrato, se ha seguido la siguiente línea de investigación:

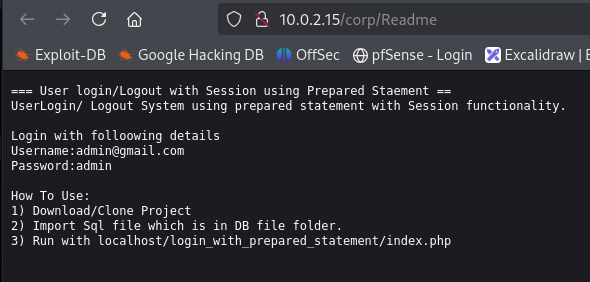
* Al no tener acceso al equipo, se procede a conectar nuestra maquina atacante (Kali) a la misma red del equipo a explotar, operando, desde ese instante, con la maquina Kali.
* A través de línea de comandos conseguimos la IP de nuestra maquina Fuzzing: 10.0.2.15 y la de la maquina atacante: 10.0.2.19.



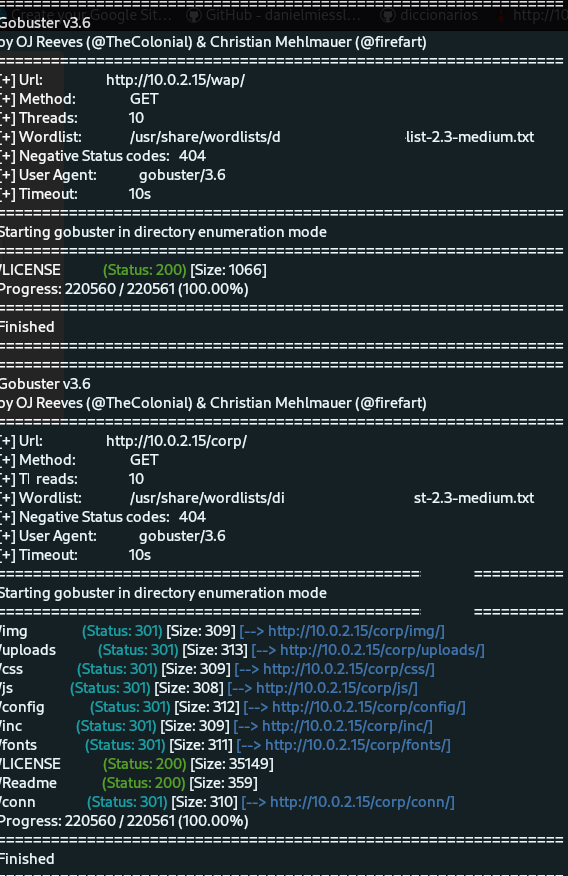
* Se usa la herramienta Dirb con la IP 10.0.2.15, obteniendo como resultado:



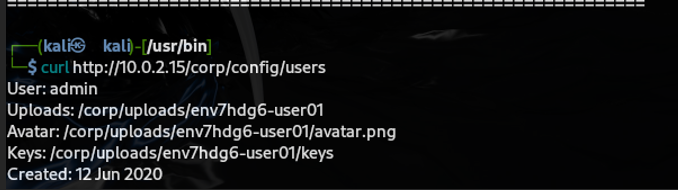
* Se accede desde el mimo navegador de nuestro equipo atacante al servidor, concretamente al directorio “*corp*” y el archivo “*Readme*”, donde se puede observar el usuario admin y la contraseña. Se prueba la misma pero no llega a funcionar, por lo que se entiende que han cambiado de contraseña del usuario admin.



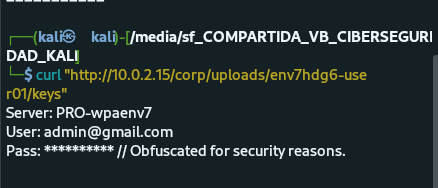
* Con la herramienta Gobuster se procede analizar el servidor en la IP 10.0.2.15, aportando todos los directorios disponibles (200). El código 301 significa que los archivos han sido removidos de manera permanente, entendiendo que se produce al conectar el servidor a la nueva red.



* Con la misma herramienta, como se ha expuesto en la introducción, al hacer un escaneo del directorio de la configuración local en el directorio *“corp”,* se encontraron credenciales y rutas de acceso a claves de usuarios:



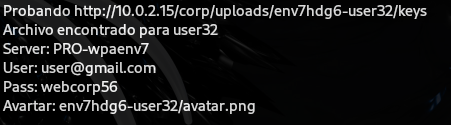
Si accedemos al directorio “*Keys”,* nos aportan credenciales del servidor, el usuario administrador del sistema y la contraseña ofuscada, por lo que se deduce que ésta se encuentra en otro directorio.



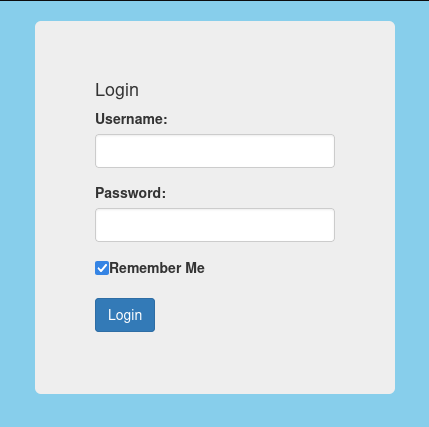
En este punto, ya podemos asegurar que el usuario es [admin@gmail.com](mailto:admin@gmail.com), ya que ha salido en distintas búsquedas en esta investigación.

Además, en el directorio *“Uploads” se* observa que al final del código terminal en *“...-user01”* , por lo que podría haber más usuarios en números correlacionados.

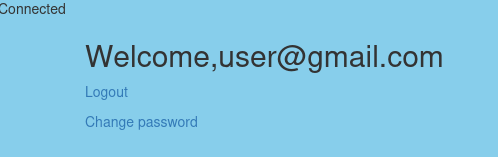
* Una vez comprobado los primeros 100 user (user01 – 100) se comprueba que el user32 existe, incorporando su usuario y contraseña:



* Ahora, que tenemos un usuario y una contraseña procedemos a intentar loquearnos en la web del servidor, la cual se encuentra protegida*:*



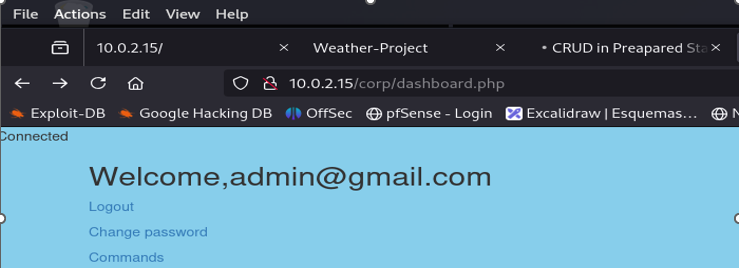
La conexión del user32 se establece de forma satisfactoria, mostrando dos pestañas, una para desconectarse y otra para cambiar la contraseña:



* En este punto, se utiliza la herramienta Burp Suite Community, que ofrece un conjunto de herramientas que trabajan juntas para apoyar todo el proceso de pruebas de seguridad, desde el mapeo inicial y el análisis de la superficie de ataque de una aplicación, hasta la identificación y explotación de vulnerabilidades de seguridad.

Con un de las funcionalidades de este programa, aprovechando el intento de cambio de clave en el user32, se procede a su escaneo, interceptando el código que ejecuta el servidor al realizar esta acción.

Una vez en Burp Suite, se procede a cambiar en línea de código el [user@gmail.com](mailto:user@gmail.com) por [admin@gmail.com](mailto:admin@gmail.com) , enviando el código modificado de vuelta al servidor, procediendo al cambio de contraseña, pero esta corresponderá al usuario [admin@gmail.com](mailto:admin@gmail.com) con privilegios root.



1. Recomendaciones generales:

Como se ha realizado un estudio, mediante la técnica del muestreo, de las principales vulnerabilidades que afectan a los dispositivos objeto de estudio, siguiendo el criterio de la criticidad, principalmente críticas, altas y medias, con la finalidad de proteger la seguridad de la empresa, la confidencialidad e integridad y disponibilidad de los datos y su adaptación a las normativas aplicables ENS, ISO 27000 y a la trasposición de la directiva europea NIS y NIS2, entre otras.

Concretamente se han expuesto y analizados un total de 16 vulnerabilidades reales, habiendo descartado las vulnerabilidades en que los dispositivos no son vulnerables por diversas causas favorables:

1. Metasploitable. – 1 de alta y 6 de media severidad.
2. Winsploitable. - 2 críticas, 4 altas y 3 de media severidad.

3.- INFORME TÉCNICO

5.- Conclusiones

Se han analizado dos dispositivos muestra de su empresa, habiendo encontrado que son vulnerables, por lo que, se recomienda implantar, por ser necesario y en la medida de lo posible, las recomendaciones indicadas para evitar daños físicos y/o digitales en los sistemas y redes de la empresa.

`gobuster` es una La herramienta opera realizando solicitudes a direcciones web con diferentes nombres, basándose en listas de palabras (wordlists), para descubrir recursos ocultos que no están enlazados en las páginas accesibles del sitio web, como directorios, archivos específicos y subdominios.

`gobuster` es apreciada por su velocidad y eficiencia, ofreciendo varias modalidades de operación, incluyendo:

- \*\*Enumeración de directorios y archivos\*\*: Permite identificar directorios y archivos en un sitio web mediante la realización de peticiones HTTP o HTTPS.

- \*\*Búsqueda de subdominios\*\*: Ayuda a encontrar subdominios válidos de un dominio específico, lo cual es útil para mapear la superficie de ataque de un objetivo.

- \*\*Enumeración de DNS\*\*: Permite la enumeración de registros DNS utilizando una técnica de fuerza bruta.

`gobuster` es una herramienta de línea de comandos y requiere que el usuario proporcione una lista de palabras que se utilizará para las pruebas de fuerza bruta. Es importante utilizar `gobuster` de manera ética y legal, generalmente con permiso explícito, para evitar acciones que puedan ser consideradas malintencionadas o ilegales.

dirb

* La herramienta realiza peticiones HTTP GET a una lista de URLs predefinidas con el objetivo de encontrar recursos accesibles en el servidor que no están enlazados desde las páginas visibles o que no deberían ser accesibles públicamente. `dirb` viene con un conjunto de listas de palabras (wordlists) que utiliza para realizar ataques de fuerza bruta contra el servidor y descubrir archivos o directorios ocultos basándose en respuestas comunes de los servidores web.
* La herramienta. Sin embargo, es importante utilizar `dirb` de manera ética y legal, generalmente con permiso explícito, para evitar acciones que puedan ser consideradas maliciosas o ilegales.

t en el sistema, utilizando herramientas diversas como Nessus, Nmap, Dirb, BurpSuite, Gobuster, entre otras, con la finalidad de informar a sus propietarios para mejorar los manuales de estrategia para la detección, contención y respuesta ante incidentes críticos en su sistema.

Burp Suite es una herramienta integrada para la seguridad de aplicaciones web, desarrollada por PortSwigger. Es ampliamente utilizada por profesionales de la seguridad para realizar pruebas de penetración y auditorías de seguridad en aplicaciones web. Burp Suite ofrece un conjunto de herramientas que trabajan juntas para apoyar todo el proceso de pruebas de seguridad, desde el mapeo inicial y el análisis de la superficie de ataque de una aplicación, hasta la identificación y explotación de vulnerabilidades de seguridad.

Las características principales de Burp Suite incluyen:

- \*\*Proxy Interceptador\*\*: Permite interceptar, inspeccionar y modificar las solicitudes y respuestas HTTP/HTTPS entre el navegador y el servidor web, facilitando el análisis detallado de las comunicaciones.

- \*\*Escáner de Vulnerabilidades\*\*: Automatiza la detección de vulnerabilidades comunes en aplicaciones web, como inyecciones SQL, cross-site scripting (XSS), y otras vulnerabilidades de seguridad web.

- \*\*Repetidor\*\*: Facilita el reenvío manual de solicitudes HTTP/HTTPS al servidor para probar cambios sutiles y observar las respuestas.

- \*\*Intruder\*\*: Automatiza ataques personalizados para encontrar y explotar vulnerabilidades de seguridad en aplicaciones web.

- \*\*Decodificador y Comparador\*\*: Herramientas para decodificar datos y realizar comparaciones entre solicitudes y respuestas, respectivamente.

Burp Suite está disponible en dos versiones: una versión gratuita con funcionalidades limitadas y una versión profesional de pago que ofrece capacidades avanzadas de escaneo de vulnerabilidades, automatización y soporte.

Es una herramienta esencial para cualquier profesional de la seguridad de aplicaciones web, proporcionando una plataforma poderosa y flexible para realizar pruebas de seguridad exhaustivas.

6.- Bibliografía

**-- Metasploitable**:

# <https://www.tenable.com/plugins/nessus/142591>

# <https://www.tenable.com/plugins/nessus/50686>

# <https://www.tenable.com/plugins/nessus/51192>

# <https://www.tenable.com/plugins/nessus/57582>

# <https://www.tenable.com/plugins/nessus/104743>

# <https://www.tenable.com/plugins/nessus/157288>

# <https://cwe.mitre.org/data/definitions/327>

# <https://www.tenable.com/plugins/nessus/187315>

# <https://terrapin-attack.com/index.html#question-answer>

# <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2023-48795>

# <https://www.tenable.com/plugins/nessus/40984/changelog>

# <https://www.tenable.com/plugins/nessus/152853>

# <https://www.tenable.com/plugins/nessus/57608>

# <https://www.tenable.com/plugins/nessus/85582>

# <https://www.tenable.com/plugins/nessus/35291>

# <https://www.tenable.com/cve/CVE-2004-2761>

# <https://www.tenable.com/cve/CVE-2005-4900>

**--Winsploitable**

# <https://www.tenable.com/plugins/nessus/125313>

# <https://www.tenable.com/cve/CVE-2019-0708>

# <https://www.tenable.com/plugins/nessus/53514>

# <https://www.tenable.com/cve/CVE-2011-0657>

# <https://www.tenable.com/cve/CVE-2011-3389>

# <https://www.tenable.com/plugins/nessus/97833>

# <https://www.tenable.com/cve/CVE-2017-0145>

# <https://www.tenable.com/cve/CVE-2017-0143>

# <https://www.tenable.com/cve/CVE-2017-0144>

# <https://www.tenable.com/cve/CVE-2017-0146>

# <https://www.tenable.com/cve/CVE-2017-0147>

# <https://www.tenable.com/plugins/nessus/97833>

# <https://www.tenable.com/plugins/nessus/35291>

# <https://www.tenable.com/plugins/nessus/42873>

# <https://www.tenable.com/cve/CVE-2016-2183>

# <https://www.tenable.com/plugins/nessus/58435>

# <https://www.tenable.com/cve/CVE-2012-0002>

# <https://www.tenable.com/cve/CVE-2012-0152>

# <https://www.tenable.com/plugins/nessus/90510>

# <https://www.tenable.com/plugins/nessus/58751>

# <https://www.tenable.com/cve/CVE-2016-0128>