



### INFORME EJECUTIVO

#### Análisis de Vulnerabilidades

- Fecha: 4 de junio de 2023
- Cliente: Iberdrola
- 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
A. Dispositivo Metasploitable	4
B. Dispositivo Winsploitable	6
4. Recomendaciones generales:	9
C. Dispositivo Metasploitable	9
D. Dispositivo Winsploitable	9
5. Conclusiones	9
6. Bibliografía	10
E. Dispositivo Metasploitable	10
F. Dispositivo Winsploitable	11

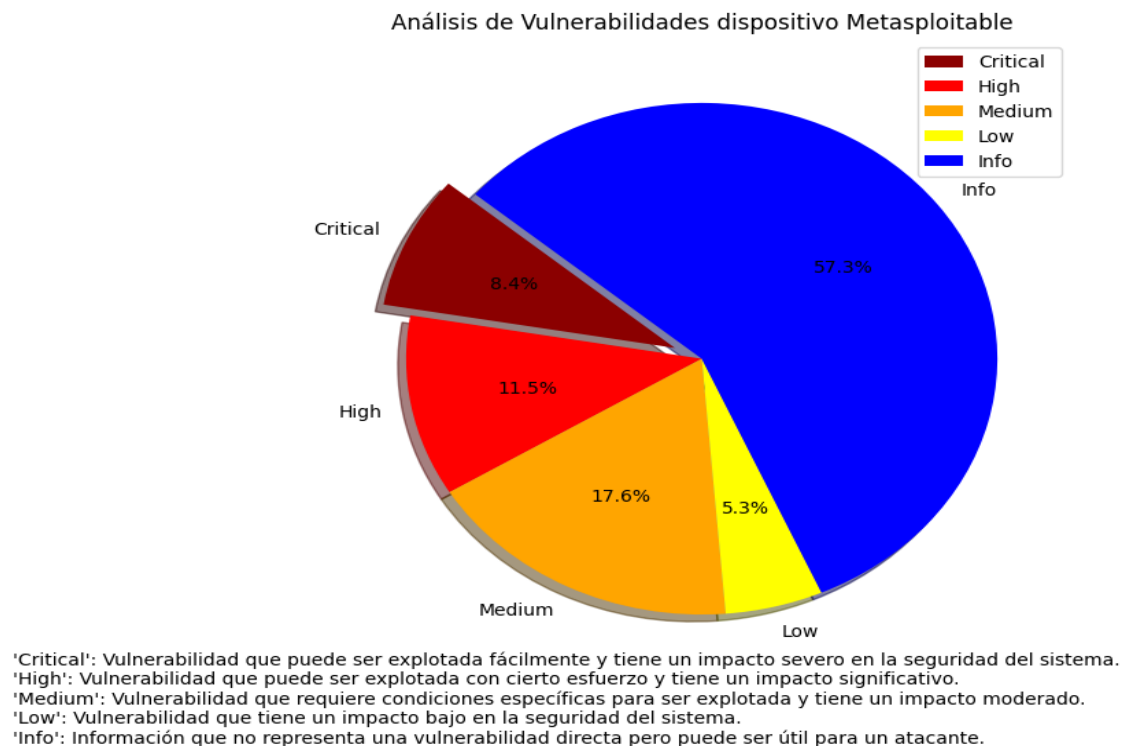
# INFORME EJECUTIVO – RETO 4

## 1. Introducción

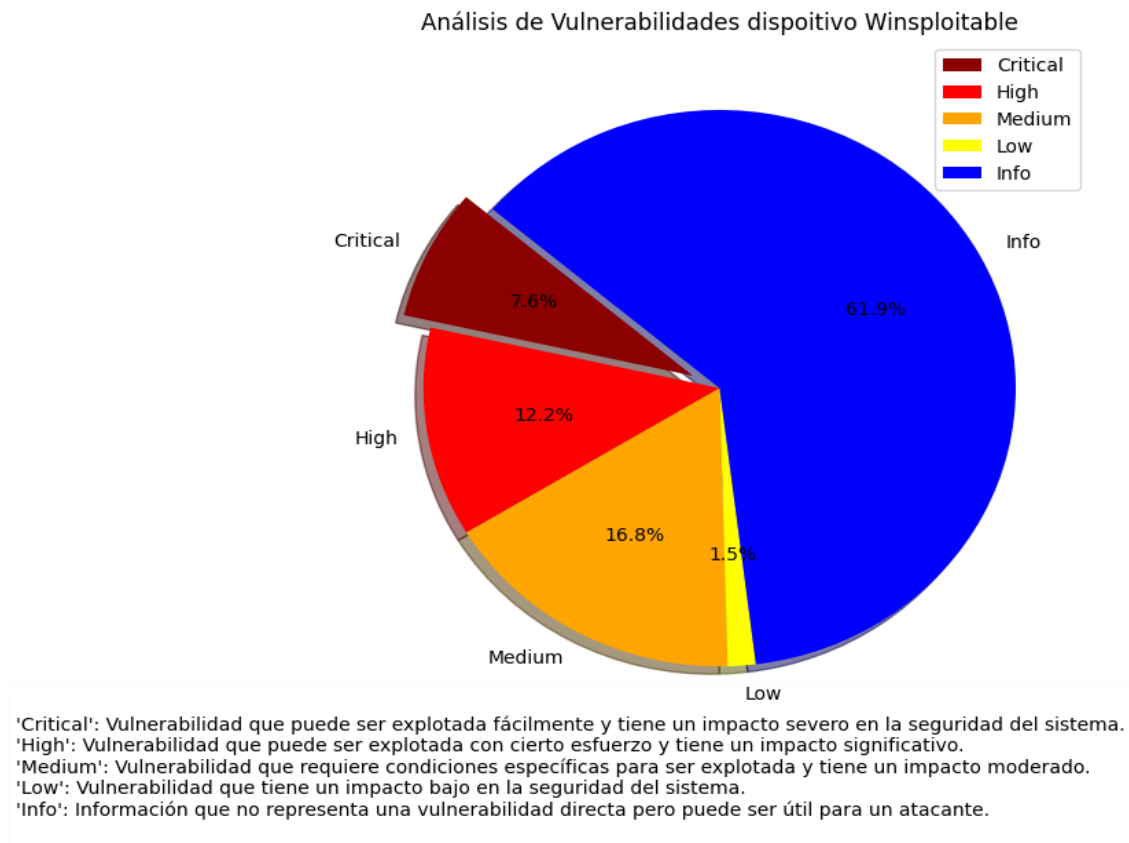
El presente informe tiene como objetivo presentar los resultados del análisis de vulnerabilidades realizado en dos equipos: Metasploitable y Windowsplotable, utilizando herramientas como Nessus y Nmap, para identificar posibles fallas de seguridad y evaluar los riesgos asociados, con la finalidad de mejorar sus manuales de estrategia para la detección, contención y respuesta ante incidentes críticos, pudiendo impedir que actores maliciosos pueden perpetrar robo de datos o daños en sus sistemas, que conllevaría una pérdida del patrimonio empresarial actual.

## 2. Alcance

El análisis de vulnerabilidades se centró en identificar y evaluar las debilidades de seguridad en los equipos mencionados, encontrando vulnerabilidades que pueden comprometer la integridad, confidencialidad y disponibilidad de los sistemas de la organización. Aquí se pueden ver el total de vulnerabilidades encontradas:



## INFORME EJECUTIVO – RETO 4

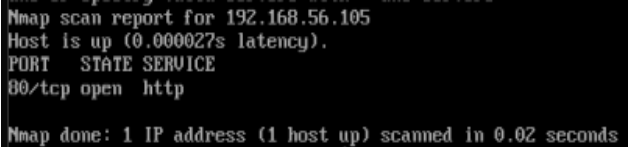


### 3. Vulnerabilidades Encontradas:

A. **Dispositivo Metasploitable.** – Este dispositivo viene con una versión de Linux Ubuntu 3.13.0, en el cual no se han identificado ninguna vulnerabilidad crítica, teniendo las protecciones necesarias en este sentido; pero si se han encontrado vulnerabilidades catalogadas de alta severidad. A continuación, se presenta un resumen de las principales vulnerabilidades y los riesgos asociados:

Vulnerabilidad detectada	Riesgo asociado	Detalles importantes a destacar
ALTA SEVERIDAD		
ID 142591 Nessus CVE-2020-7071 CVE-2020-7072 CVE-2020-7074 CVE-2020-7075	<u>PHP &lt; 7.3.24 Multiple Vulnerabilities:</u> La versión PHP inferior a la versión 7.3.24 es afectado por múltiples vulnerabilidades, permitiendo ataques de DoS	Según la web “php.net”, la versión que menos vulnerabilidades tiene es la 7.4.33, existiendo versiones 8.0, las cuales presentan muchas vulnerabilidades, no existiendo exploits públicos conocidos En esta web se puede ver el código PHP vulnerable: <a href="https://vulners.com/nessus/PHP_7_3_24.NASL">https://vulners.com/nessus/PHP_7_3_24.NASL</a>

## INFORME EJECUTIVO – RETO 4

SEVERIDAD MEDIA		
CVE-1999-05011 (actualizado en 2017) ID Nessus 50686	<u>IP Forwarding Enabled</u> Permite enrutar paquetes de datos a través del dispositivo del atacado, eludiendo firewall/Routers/filtrado MAC	Si esta activado el servidor remoto, deshabilitar el reenviado de IPs a través del puerto 80. Maquina Metasploitable: 
ID Nessus ID 104743 CVE-2008-3775 CVE-2007-4150 CVE-2007-5460 CVE-2005-4860 CVE-2002-2058 CVE-2008-2188 CVE-2005-2946 CVE-2007-6013 CWE-327	<u>SSL Certificate Cannot Be Trusted:</u> Puede facilitar la realización de ataques “Man in the Middle”, vulnerando los certificados de confianza para aplicaciones de seguridad (web)	Impacta sobre la confidencialidad e integridad de los datos, si el algoritmo criptográfico se usa para asegurar la identidad de la fuente de los datos (como las firmas digitales), entonces un algoritmo roto comprometerá este esquema y la fuente de los datos no puede ser certificada, no teniendo exploits públicos.
Nessus ID 57582	<u>SSL Self-Signed Certificate:</u> Similar al anterior, La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido.	Este plugin no comprueba las cadenas de certificados que terminan en un “no autofirmado”, y en estos casos, puede estar firmado por una autoridad de certificación no reconocida, no encontrando exploits públicos para su explotación. Se recomienda el uso de certificados criptográficos de entidades públicas de confianza.
Nessus ID 152853 IAVT: 0001-T-0936	<u>PHP &lt; 7.3.28 Email Header Injection:</u> Un atacante puede manipular las cabeceras de un email, enviado desde una web, permitiendo a éste, enviar emails maliciosos o spam desde el servidor de la víctima.	Un servidor web afectado por esta vulnerabilidad que tenga un formulario de contacto, que permita a los usuarios enviar emails sin controlar entradas o escapadas, pueden perder el control de su email.  Por ello, se recomienda actualizar a la versión superior de PHP, para no perder el control total del contenido de los encabezados del correo electrónico.

## INFORME EJECUTIVO – RETO 4

<p>Nessus ID 47831</p> <p>CWE: 116, 20, 442442, 692, 712712, 722, 725725, 74, 751751, 79, 80, 801801, 811, 811811, 83, 84, 85, 86, 87, 928, 931</p>	<p><u>CGI Generic XSS (comprehensive test):</u></p> <p>Esta vulnerabilidad realiza ataques scripting (XSS) a los servidores web remotos que albergan scripts CGI rotos, que no logran controlar las entradas (valida o escapa) de los usuarios antes de reflejarla en la salida del HTML.</p>	<p>La solución es restablecer el acceso a la aplicación vulnerable y actualizar o parchear por el soporte técnico, no existiendo exploits públicos disponibles.</p>
<p>Nessus ID 85582</p> <p>CVE 693</p>	<p>Web Application Potentially Vulnerable to Clickjacking:</p> <p>un atacante engaña a un usuario para que haga clic en algo diferente de lo que el usuario percibe, lo que puede llevar a acciones no deseadas, como cambiar configuraciones, realizar compras, o incluso ejecutar comandos maliciosos. Esto se logra superponiendo un elemento transparente o semitransparente sobre un enlace o botón legítimo.</p>	<p>Implementar medidas, como la directiva “frame-ancestors”, evitando que el contenido de la pagina sea renderizado por un sitio malicioso. No se han encontrado exploits públicos.</p>

**B. Dispositivo Winsploitable:** Este dispositivo cuenta con el Windows Server 2008 R 2 standard, en el cual se han identificado vulnerabilidades críticas, alta y media severidad. A continuación, se presenta un resumen de las principales vulnerabilidades y los riesgos asociados:



## INFORME EJECUTIVO – RETO 4

Vulnerabilidad detectada	riesgo	Detalles importantes a destacar
<b>SEVERIDAD CRÍTICA</b>		
<p>Nessus ID 125313</p> <p>Nessus ID 42873</p> <p>CVE- 2019-0708</p>	<p><u>Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed Check):</u></p> <p>Permite a un atacante ejecutar código malicioso de manera remota, pudiendo acceder y hacer capturar de pantallas, inclusive</p>	<p>Tiene un factor de riesgo muy alto por lo que debe solucionarse lo antes posible, afectando al protocolo de escritorio remoto de Windows (RCP). Existen exploits públicos que permiten ejecutar esta vulnerabilidad a través de herramientas de explotación de vulnerabilidades.</p> <p>Actualizar a través de la web de Microsoft para aplicar el parche de seguridad.</p>
<p>Nessus ID 53514</p> <p>CVE-2011-0657</p>	<p>MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check):</p> <p>Ataque remoto aprovechando las resoluciones de los servidores DNS de Windows en el sistema.</p>	<p>Es una vulnerabilidad muy crítica, por lo que es urgente su resolución, consistente en la instalación de los parches de seguridad de Microsoft. Existen exploits públicos vulnerables a través de aplicaciones de explotación de vulnerabilidades.</p>
<b>SEVERIDAD ALTA</b>		
<p>Nessus ID 97833</p> <p>CVE-2017-0144</p> <p>CVE-2017-0143</p> <p>CVE-2017-0146</p> <p>CVE-2017-0147</p> <p>CVE-2017-0148</p>	<p>MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check):</p> <p>Presenta múltiples vulnerabilidades por ataque de divulgación de la información a través del protocolo SMB, además puede ser explotado por el Ransomware WannaCry, entre otros</p>	<p>Es una vulnerabilidad con una puntuación que roza ser crítica, sin embargo, en urgencia de resolución tiene una puntuación de 9.7, por lo que se recomienda tomar medidas inmediatas, mediante las actualizaciones y parches disponibles en Microsoft.</p> <p>Aunque sea considerada de alta severidad, es crítica por la urgencia, debido a la amenaza de WannaCry al sistema, siendo unas de las vulnerabilidades que se encuentra dentro de las mas importantes dentro de la historia de la Ciberseguridad.</p>

## INFORME EJECUTIVO – RETO 4

<p>Nessus ID 35291</p> <p>CVE-2004-2761</p> <p>CVE-2005_4900</p>	<p>SSL Certificate Signed Using Weak Hashing Algorithm:</p> <p>Aprovechan la debilidad de los métodos de encriptación MD5 y SHA1 entre otros, para conseguir falsear un hash idéntico al original, comprometiendo la confidencialidad e integridad de los datos.</p> <p><u>SSL Medium Strength Cipher Suites Supported (SWEET32):</u></p> <p>Nessus considera SSL de resistencia media los cifrados que usen entre 64 a 112 bits o el 3DES</p>	<p>Los atacantes realizan ataques por colisión, siendo un tipo de ataque criptográfico donde se encuentran dos entradas diferentes que producen el mismo hash, pudiendo falsificar un certificado SSL.</p> <p>Si sospecha de algo, Se recomienda contactar con la entidad publica de certificados para que emita otro, ya que existen exploits públicos que pueden realizar estas acciones, evitando ataques Sweet32, que explotan esta debilidad. Se recomienda el uso de cifrados de 128bit en adelante.</p>
<p>Nessus ID 58435</p> <p>CVE-2012-0002</p> <p>CVE-2012-0152</p>	<p><u>MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check):</u></p> <p>Ejecución de código no autorizado a través del protocolo de escritorio remoto de Windows por un fallo en la forma que RDP procesa los paquetes en la memoria, pudiendo causar una denegación de los servicios.</p>	<p>Se recomienda actualizar los parches publicados por Microsoft rápidamente, ya que, aunque sea una severidad considerada alta, en la valoración de la urgencia en su resolución es como si fuera crítica, con una puntuación de 9.6. Además, existen exploits públicos que pueden explotar esta vulnerabilidad.</p>
<b>SEVERIDAD MEDIA</b>		
<p>Nessus ID 90510</p> <p>CVE-2016-0128</p>	<p>MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock)</p> <p>(uncredentialed check):</p> <p>Un atacante podría realizar un ataque MITM, forzando acceso al sistema y elevando privilegios aprovechando</p>	<p>Este ataque “Man in the Middle” ataca a las interfaces de comunicación utilizadas en sistemas Windows para acceder a información de seguridad y administración (SAM y LCD), siendo recomendable actualizar con el conjunto de parches lanzado por Microsoft. No existen exploits públicos conocidos para su explotación.</p>



## INFORME EJECUTIVO – RETO 4

	vulnerabilidades los canales SAM y LCD.	
Nessus ID 58751	<u>SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST):</u> Permite ataques de divulgación de la información, en caso de utilizar conexiones remotas SSL/TLS en versiones 1.0 y 3.0	Se recomienda configurar los servidores con los protocolos de seguridad TLS 1.1 o 1.2 que no usan cifrado en bloque, existiendo un parche de actualización de Microsoft para su corrección automática (KB2643584). No existen exploits públicos conocidos

### 4. 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:

C. Metasploitable. – 1 de alta y 6 de media severidad.

D. Winsploitable. - 2 críticas, 4 altas y 3 de media severidad.

### 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.

### 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>