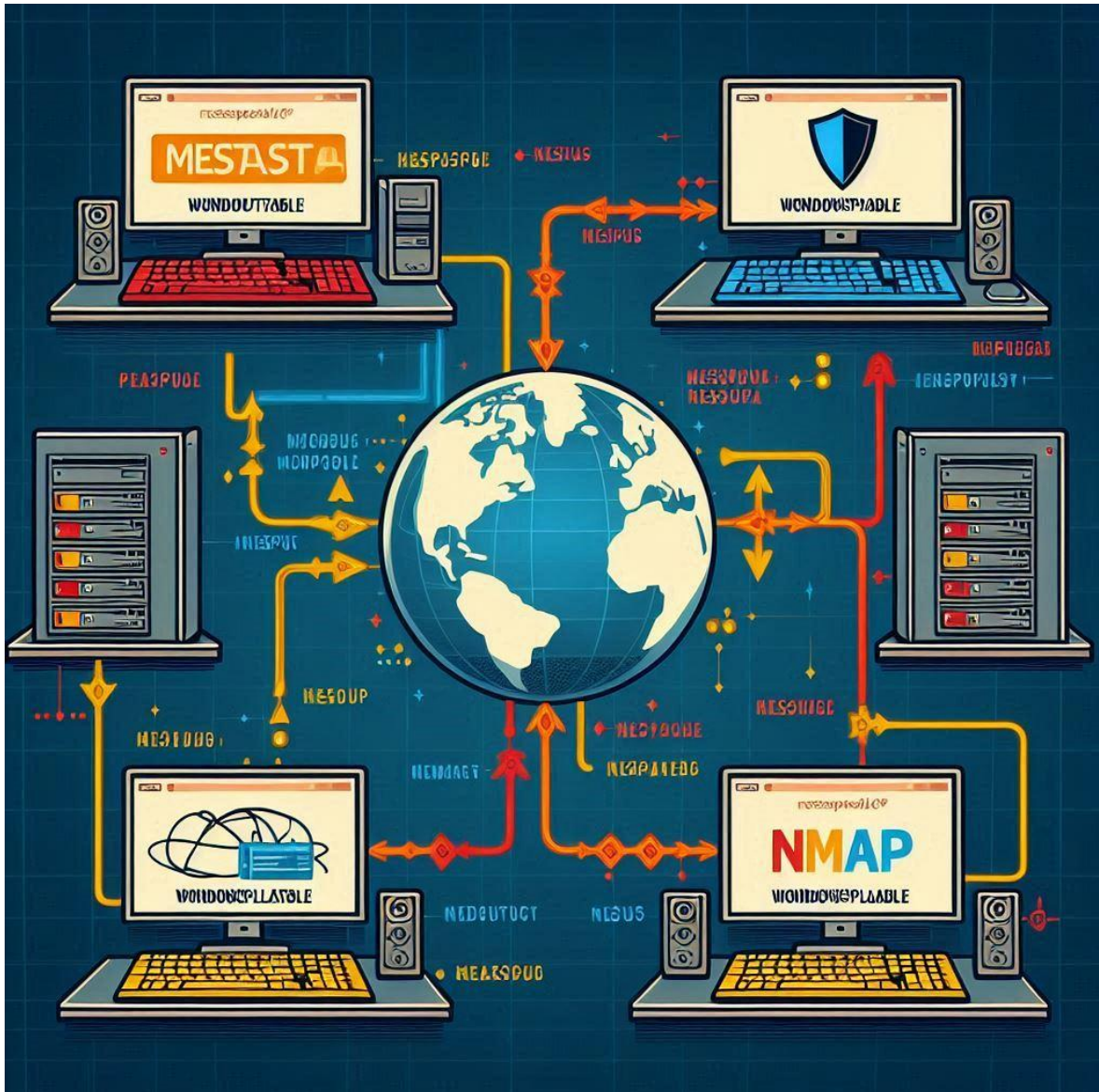


INFORME TÉCNICO – RETO 4



INFORME TÉCNICO

Análisis de Vulnerabilidades

- Fecha: 4 de julio 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

INFORME TÉCNICO – RETO 4

Índice de Contenidos

1. Introducción	3
2. Alcance	3
3. Vulnerabilidades encontradas:	4
A. Dispositivo Metasploitable	4
B. Dispositivo Winsploitable	10
4. Soluciones o Recomendaciones:	17
C. Dispositivo Metasploitable	17
D. Dispositivo Winsploitable	17
5. Conclusiones	17
6. Bibliografía	18
E. Dispositivo Metasploitable	18
F. Dispositivo Winsploitable	19

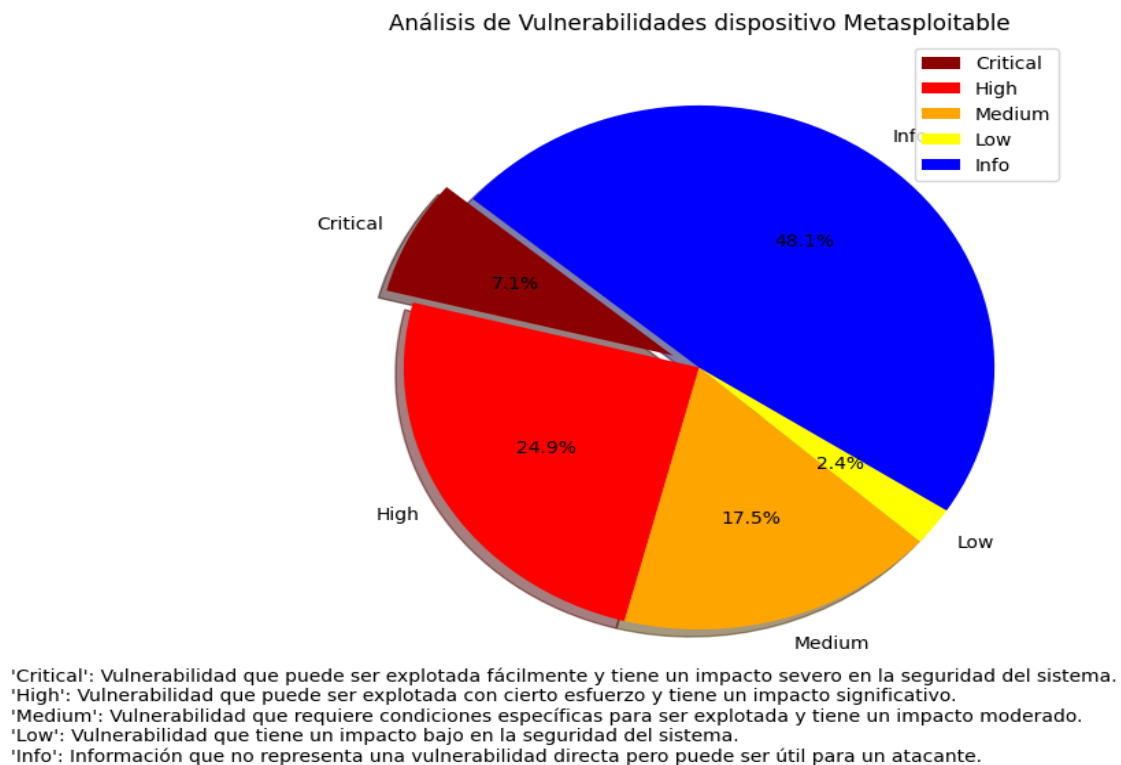
INFORME TÉCNICO – RETO 4

1. Introducción

Este informe técnico presenta un análisis exhaustivo de las vulnerabilidades identificadas en los hosts: Metasploitable y Windowsplotable. Para llevar a cabo este análisis, se emplearon herramientas avanzadas de ciberseguridad, incluyendo Nessus para la detección de vulnerabilidades y Nmap para el reconocimiento de puertos y servicios. El objetivo de este informe es proporcionar una evaluación detallada de las debilidades de seguridad encontradas, así como los riesgos potenciales que estas vulnerabilidades representan para la integridad, confidencialidad y disponibilidad de los sistemas de la organización.

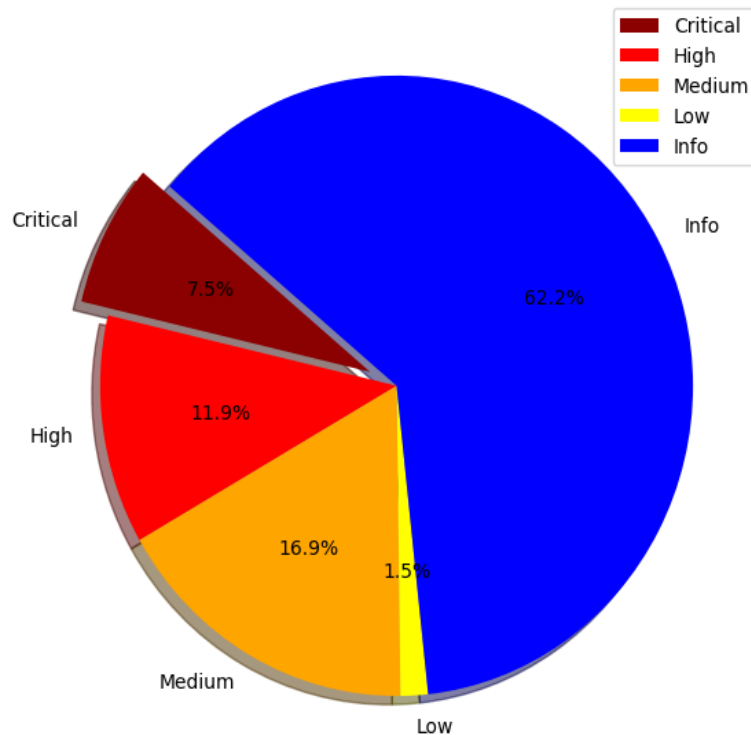
2. Alcance

El análisis abarcó la identificación de vulnerabilidades que podrían ser explotadas por atacantes para comprometer la seguridad de los sistemas, representando un riesgo significativo para la organización y afectando la integridad, confidencialidad y disponibilidad de los datos, así como daños físicos y/o digitales que pudieran provocar en sistemas y redes de la organización. Aquí se pueden ver el total de vulnerabilidades encontradas:



INFORME TÉCNICO – RETO 4

Análisis de Vulnerabilidades dispositivo Winsploitable



'Critical': Vulnerabilidad que puede ser explotada fácilmente y tiene un impacto severo en la seguridad del sistema.

'High': Vulnerabilidad que puede ser explotada con cierto esfuerzo y tiene un impacto significativo.

'Medium': Vulnerabilidad que requiere condiciones específicas para ser explotada y tiene un impacto moderado.

'Low': Vulnerabilidad que tiene un impacto bajo en la seguridad del sistema.

'Info': Información que no representa una vulnerabilidad directa pero puede ser útil para un atacante.

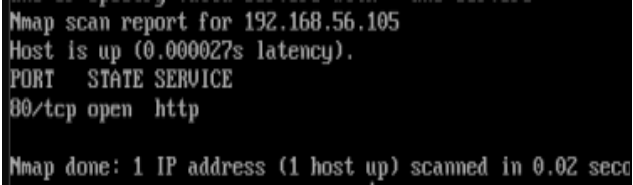
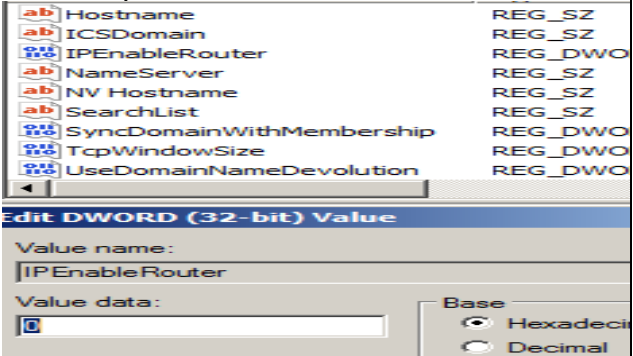
3. Vulnerabilidades Encontradas

A continuación, se detallan las vulnerabilidades identificadas, siguiendo el criterio criticidad y las soluciones recomendadas:

- Dispositivo Metasploitable:**

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 < 7.3.24</u> <u>Multiple Vulnerabilities:</u> La versión PHP inferior a la versión 7.3.24 es afectado por múltiples vulnerabilidades, permitiendo ataques de DoS	Presenta un CVSS de 7.5 y un VPR de 5.0, afectado a la aplicación PHP. 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 para su explotación. La información ha sido actualizada el 4 de junio de 2024, afectado al puerto 80/www

INFORME TÉCNICO – RETO 4

SEVERIDAD MEDIA		
<p>CVE-1999-05011 (actualizado en 2017)</p> <p>ID Nessus 50686</p>	<p>IP Forwarding Enabled Cuando el reenvío de IP está habilitado, el dispositivo puede reenviar paquetes de datos entre diferentes interfaces de red, actuando efectivamente como un router. Esto puede ser explotado por un atacante para eludir medidas de seguridad como firewalls, Routers y filtrado de direcciones MAC.</p> <p>Em caso que un atacante, pueda activar este servicio en un dispositivo comprometido podrá eludir las reglas del firewall, hacer un bypass de Routers usando rutas no autorizadas y evitando las restricciones de MAC, ya que el reenvío va con un MAC autorizada</p>	<p>Si esta activado el servidor remoto, deshabilitar el reenviado de IPs a través del puerto 80. Maquina Metasploitable tiene el puerto abierto y esta activado:</p>  <p>La solución reside en desactivar el ip-forward, de la siguiente forma dependiendo del sistema operativo:</p> <p>-Linux: <code>echo 0 - /proc/sys/net/ipv4/ip-forward</code></p> <p>-Windows: HKEY-LOCAL-MACHINE-System-CurrentControlSet-Services-Tcpip-Parameters</p> <p>-MAC OS X: <code>sysctl -w net.inet.ip.forwarding=0</code>.</p> <p>En Winsploitable está desactivado:</p>  <p>Pero puede ser activado remotamente por actores maliciosos, debiendo estar el tráfico de red monitoreado con dispositivos IDS/IPS o EDS para controlar esta vulnerabilidad.</p>

INFORME TÉCNICO – RETO 4

<div>ID Nessus ID 51192</div> <div>CVE-2008-3775</div> <div>CVE-2007-4150</div> <div>CVE-2007-5460</div> <div>CVE-2005-4860</div> <div>CVE-2002-2058</div> <div>CVE-2008-2188</div> <div>CVE-2005-2946</div> <div>CVE-2007-6013</div> <div>CWE-327</div>	<div><u>SSL Certificate Cannot Be Trusted y SSL Self-Signed Certificate</u></div> <div>Estas dos vulnerabilidades están relacionadas y pueden facilitar la realización de ataques “Man in the Middle”, vulnerando los certificados de confianza tipo certificado X.509.</div> <div>Este certificado es un estándar de formato para los certificados de clave pública. Estos certificados se utilizan en diversas aplicaciones de seguridad, como SSL/TLS para sitios web seguros.</div>	<div>Esta debilidad podría facilitar la realización de ataques por actores maliciosos tipo “MITM”, habida cuenta que, usando certificados vulnerables, se puede romper la cadena de confianza de las siguientes formas:</div> <div><ul style="list-style-type: none">El encabezado del certificado enviada al servidor podría ser un certificado no reconocido y autofirmado, o pueden faltar certificados intermedios que conecten con el encabezado de un certificado de autoridad pública.Cuando se escanea el certificado antes de una de las fechas de inicio en el campo “NotBefore” del certificado o después de las fechas del campo “NotAfter” del mismo, pudiendo contener certificados no valido.La cadena de certificados puede contener una firma que no coincida con la información del certificado, o no pudo ser verificado.</div> <div>Para impedir esto se recomienda generar certificados SSL adecuados, así como asegurarse de que el reloj del sistema esté correctamente sincronizado con un servidor de tiempo confiable (NTP) y monitorear las fechas de expiración de los certificados y renovación antes de que expiren, encontrándose una renovación corregida con fecha de octubre de 2023:</div>
--	---	---

Recommendation X.509 (2019) Corrigendum 2 (10/23)

Approved in 2023-10-29

Status : In force

Access : Free Download

Available languages and formats :

Click on the selected format and language to get the document

Format	Size	Posted	Article Number
English <div><div><div></div><div></div></div> Word 2007</div>	94281 bytes	2023-11-28	E 80000
<div><div><div></div><div></div></div> PDF (acrobat)</div>	352052 bytes	2023-11-28	

INFORME TÉCNICO – RETO 4

<p>Nessus ID 152853</p> <p>IAVT: 0001-T-0936</p>	<p>PHP < 7.3.28</p> <p>Email Header Injection:</p> <p>ejecuta en el servidor web remoto una inyección de encabezado de correo electrónico, si tiene una versión anterior de PHP citada. En versiones de PHP anteriores a 7.3.28, la función <i>imap_mail_compose</i> no valida adecuadamente los encabezados de correo electrónico, lo que permite la inyección de los encabezados, lo que puede llevar a la manipulación del contenido del correo y a la explotación de la vulnerabilidad.</p>	<p>Esta se produce debido a un fallo en el manejo de las secuencias de CR-LF en los campos de encabezado, aprovechando esta situación actores maliciosos para insertar caracteres en la línea de encabezados del correo electrónico, obteniendo un control total del contenido de dichos encabezados, siendo su solución actualizar a la versión indicada anteriormente o superior de PHP y cambiando la opción “habilitar CGI escaneado” a la opción “true” (modificación del 4 de junio de 2004).</p> <p>Como prueba del modo en que la versión PHP puede ser modificada maliciosamente para inyección de los encabezados maliciosos, podemos usar un código que cree un correo electrónico “multipart” con varias partes (texto plano y un archivo binario) y lo compone utilizando la función <i>imap_mail_compose</i>. Los encabezados del correo y las partes del mensaje contienen texto adicional From: X-INJECTED, lo que sugerirá que el código podría estar probando la inyección de encabezados en correos electrónicos.</p> <p>Se recomienda actualizar la versión PHP para no perder el control total del contenido de los encabezados del correo electrónico.</p>
		<pre><?php \$envelope["from"] = "joe@example.com\n From : X-INJECTED"; \$envelope["to"] = "joe@example.com\nFrom: X-INJECTED"; \$envelope["cc"] = "bar@example.com\nFrom: X-INJECTED"; \$envelope["subject"] = "bar@example.com\n\n From : X-INJECTED"; \$envelope["x-remail"] = "bar@example.com\nFrom: X-INJECTED"; \$envelope["something"] = "bar@example.com\nFrom: X-INJECTED"; \$part1["type"] = TYPEMULTIPART; \$part1["subtype"] = "mixed"; \$part2["type"] = TYPEAPPLICATION; \$part2["encoding"] = ENCBINARY; \$part2["subtype"] = "octet-stream\nContent-Type: X-INJECTED"; \$part2["description"] = "some file\nContent-Type: X-INJECTED"; \$part2["contents.data"] = "ABC\nContent-Type: X-INJECTED"; \$part3["type"] = TYPETEXT; \$part3["subtype"] = "plain"; \$part3["description"] = "description3"; \$part3["contents.data"] = "contents.data3\n\n\n\t"; \$body[1] = \$part1; \$body[2] = \$part2; \$body[3] = \$part3; echo imap_mail_compose(\$envelope, \$body); ?></pre>

INFORME TÉCNICO – RETO 4

<p>Nessus ID 47831 CWE: 116, 20, 442442, 692, 712712, 722, 725725, 74, 751751, 79, 80, 801801, 811, 811811, 83, 84, 85, 86, 87, 928, 931</p>	<p>CGI Generic XSS (comprehensive test):</p> <p>Esta vulnerabilidad realiza ataques scripting (XSS) a los servidores web remotos que albergan scripts CGI rotos, que no logran desinfectar adecuadamente , siendo necesario para prevenir este tipo de vulnerabilidades , desinfectar y validar todas las entradas del usuario, incluyendo:</p> <p>-Escapar caracteres especiales: Convertir caracteres como <, >, &, etc., en sus entidades HTML semejantes.</p> <p>-Usar bibliotecas de seguridad: Utilizar bibliotecas y frameworks que proporcionen funciones de desinfección y</p>	<p>Esta vulnerabilidad presenta una severidad de 4.3, sin puntuación de urgencia en resolución, donde servidores web pueden ser propensos a ataques XSS no persistentes, el cual consiste en aprovechar que los scripts CGI de la web no logran desinfectar adecuadamente las cadenas de solicitud de scripts malicioso, pudiendo ser capaces actores maliciosos de hacer que el código HTML y el script se ejecuten de forma conjunta en el navegador de un usuario dentro del contexto de seguridad del sitio web afectado</p> <p>Scripting Cross-site (XSS) es una técnica de ataque que implica un atacante consigue que el navegador de un usuario ejecute su código, el código se ejecutará dentro del sitio web de alojamiento. Con este nivel de privilegio, el código tiene la capacidad de leer, modificar y transmitir cualquier dato sensible accesible por el navegador de un usuario. El script en el sitio web controlado por el atacante podría tener su cuenta secuestrada (robo de cookies), su navegador redirigido a otra ubicación, o posiblemente mostrar contenido fraudulento entregado por el sitio web que está visitando. Además, hace de espejo del sitio web remoto y puede extraer la lista de CGI que son utilizados por el usuario remoto.</p> <p>En este caso estamos ante un script XSS de tipo “no persistente”. Supongamos que tenemos un script CGI (Common Getaway Interface: Tecnología que permite a los servidores interactuar con programas externos(scripts))) que toma como parámetro “name” de la URL, es decir, si un atacante incluyera en la URL con un script malicioso:</p> <p style="text-align: center;"><u><a href="http://example.com/cgi-bin/hello.cgi?name=<script>alert('XSS')</script>">http://example.com/cgi-bin/hello.cgi?name=<script>alert('XSS')</script></u></p> <p>Donde XSS es el código malicioso:</p>
--	---	--

INFORME TÉCNICO – RETO 4

	<p>validación de entradas.</p> <p>-Políticas de Seguridad de Contenidos (CSP): Implementar CSP para restringir la ejecución de scripts no autorizados.</p>	<p>XSS="<html><body>Hello, <script>alert('XSS')</script>!/body></html>"(imagen_1)</p> <p>Si el usuario visita la web, el XSS se ejecutará en su navegador y en este caso mostraría una alerta, pero en caso reales, podría robarle la cuenta de ese sitio web, entre otras. (imagen_2)</p> <p>La solución es restablecer el acceso a la aplicación vulnerable, validar y escapar de todas las entradas de usuario (imagen_3) y actualizar o parchear por el soporte técnico. No existen exploits públicos disponibles</p> <p>Imagen_1</p>
--	--	--

```
#!/usr/bin/perl
print "Content-type: text/html\n\n";
my $$name = $$ENV{'QUERY_STRING'};
print "<html><body>Hello, $name!</body></html>";
```

Imagen_2

```
<html>
<body>Hello, <script>alert('XSS');</script>!/body>
</html>
```

Imagen_3

```
#!/usr/bin/perl
use strict;
use warnings;
use CGI;
use HTML::Entities;

print "Content-type: text/html\n\n";

my $$query = CGI->new;
my $$name = $$query->param('name');
$$name = encode_entities($$name);

print "<html><body>Hello, $name!</body></html>";
```

INFORME TÉCNICO – RETO 4

<p>Nessus ID 85582</p> <p>CVE 693</p>	<p>Web Application Potentially Vulnerable to Clickjacking: Un atacante puede engañar a un usuario de la web para que haga click en una parte de web que es maliciosa, resultando finalmente ser víctima de una estafa.</p>	<p>Esta vulnerabilidad para Linux y Windows, presenta una severidad de 4.3 de puntuación, sin tener valor alguno en cuanto a la urgencia de su resolución. Si se ejecuta en un servidor web remoto que no tiene configurado la cabecera de respuesta adecuadamente, expone el sitio web a un ataque de “clickjacking”, en el que actores maliciosos pueden engañar a los usuarios de la web, para que al hacer click en una zona de la página que han vulnerado, esta realice acciones fraudulentas o maliciosas sobre el mismo, las cuales, el usuario no es capaz de percibir en la zona de la web.</p> <p>Los métodos X-Frame-Options y Content-Security-Policy o Frame-ancestors, no son los únicos que pueden evitar este tipo de ataques, existiendo actualmente métodos más confiables a través de la automatización, pero que pueden generar falsos positivos si se despliegan junto a otras estrategias.</p> <p>La solución a esta vulnerabilidad es devolver el encabezado HTTP con alguno de estos métodos mencionados, con la respuesta de la página web, evitando que el contenido sea renderizado por otra web cuando utilice el marco o las etiquetas HTML.</p>
---	--	--

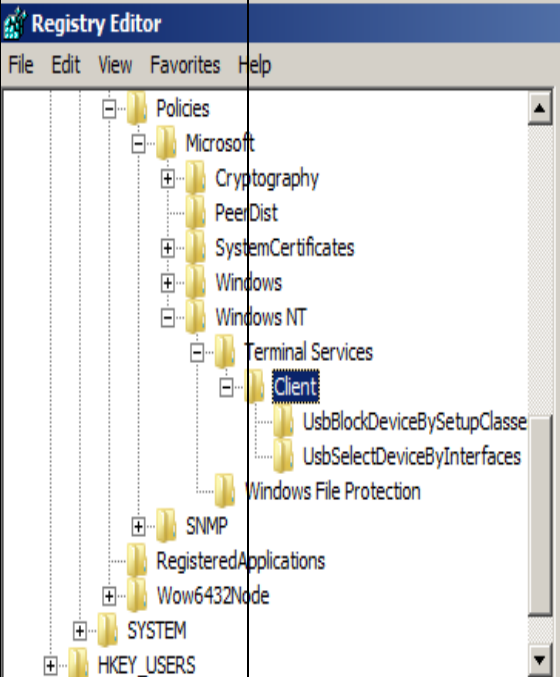
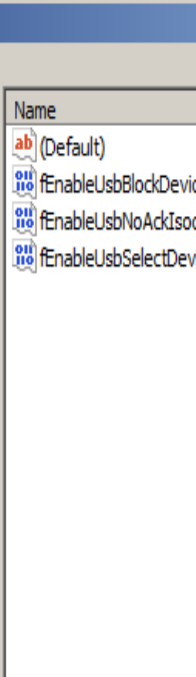
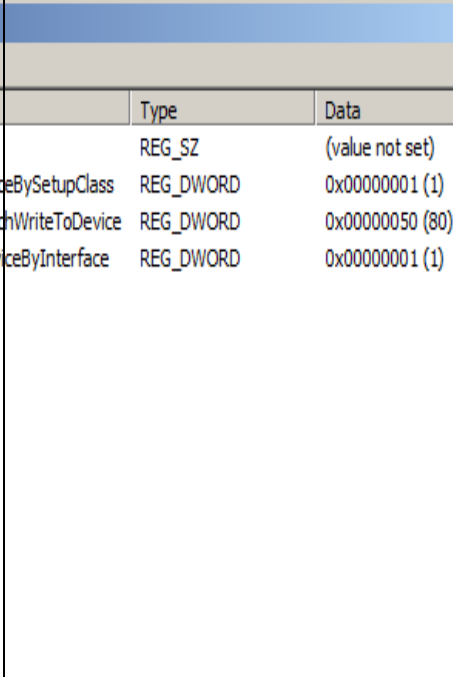
• Dispositivo Winsploitable:

Vulnerabilidad detectada	riesgo	Detalles importantes a destacar
SEVERIDAD CRÍTICA		
<p>Nessus ID 125313</p> <p>Nessus ID 42873</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 al dispositivo del usuario, siendo necesarias unas medidas preventivas tener todas las aplicaciones actualizadas de</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), existiendo exploits públicos que permiten ejecutar esta vulnerabilidad a través de herramientas de</p>

INFORME TÉCNICO – RETO 4

<p>CVE- 2019-0708</p>	<p>productos Microsoft, aunque no las use y no desee desinstalarlas, ya que es un vector de ataque para su dispositivo y sus datos.</p> <p>Como posibles soluciones a esta vulnerabilidad con un CVSS de 10 y VPR de 9.7 son:</p> <ol style="list-style-type: none"> 1. Habilitar la autenticación a Nivel de Red (NLA), método que mejora la seguridad de las conexiones de escritorio remoto al requerir que el usuario se autentique / autenticación y credenciales) antes de establecer una sesión completa de RDP. Aplicarlo en los sistemas que ejecutan ediciones compatibles de Windows 7, Windows Server 2008 y Windows Server 2008 R2 2. Bloqueo del puerto predeterminado en el cortafuegos perimetral de la empresa para RDP: TCP 3389. <p>Si es necesario el uso del acceso remoto, hay que considerar opciones complementarias de seguridad como la instalación de VPN que tunelizan y encriptan las comunicaciones.</p> <p>Bloquear los puertos afectados en el perímetro de la empresa es la mejor defensa para ayudar a evitar ataques basados en Internet. Sin embargo, los sistemas todavía podrían ser vulnerables a los ataques desde dentro de su perímetro empresarial, por lo que es necesario, EL uso de medias complementarias de seguridad para el cifrado y encriptado seguro de las comunicaciones y monitorizar alertas (IDS, IPS, EDR, Firewal, etc.).</p>	<p>explotación de vulnerabilidades.</p> <p>Esta vulnerabilidad de ejecución de código remoto en Remote Desktop Services (RCP), antes conocido como "Terminal Services", donde un atacante no autenticado se conecta al sistema de destino utilizando RDP y envía peticiones especialmente elaboradas, podría ejecutar código arbitrario en el sistema de destino. no requiriendo interacción del usuario afectado, pudiendo en este caso: instalar programas; ver, cambiar o eliminar datos; o crear nuevas cuentas con plenos derechos de usuario.</p> <p>Para explotar esta vulnerabilidad, un atacante tendría que enviar una solicitud especialmente elaborada a los sistemas de destino Servicio de Escritorio Remota a través de RDP.</p>
-----------------------	---	---

INFORME TÉCNICO – RETO 4

<p>Nessus ID 53514</p> <p>CVE-2011-0657</p>	<p><u>MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check):</u></p> <p>Ataque remoto aprovechando las resoluciones locales de nombres (similar al DNS) de Windows en el sistema, siendo necesaria una urgente actualización con parches de Microsoft.</p> <p>En el dispositivo objeto de estudio se comprueba que no tiene la "EnableMulticast", por lo que está activado por defecto (como si tuviera 1). Para deshabilitarlo, es necesario crear la clave anteriormente mencionada en la ruta del registro de Windows de Hkey_Local_Machine/.../Windows NT\DNSClient' y proporciónale el valor 0.</p>	<p>Es una vulnerabilidad muy crítica, con una CVSS de 10 y un VPR de 7.3, por lo que es urgente su resolución.</p> <p>Existen exploits públicos capaces de explotar esta vulnerabilidad, que afecta al protocolo LLMNR (Link Local Multicast Name Resolución), el cual, permite la resolución de nombres en redes pequeñas locales sin necesidad de un servidor DNS, a través del cual, un atacante dentro de la red local puede enviar una respuesta código malicioso de consulta al LLMNR, ejecutándose en el contexto de la cuenta que utiliza Windows (NetworkService) permitiendo interactuar en la red con ciertas limitaciones, pero permitiendo movimientos laterales del atacante dentro de ella.</p> <p>Para su mitigación es conveniente deshabilitar el LLMNR, si no es necesario, monitorizar la red y tener el software actualizado.</p>
		

INFORME TÉCNICO – RETO 4

SEVERIDAD ALTA		
Nessus ID 97833	<u>MS17-010: Security Update for Microsoft Windows SMB Server (4013389)</u>	<p>Es una vulnerabilidad, se encuentra dentro de las más conocidas en la historia de la ciberseguridad. Aunque tiene una puntuación que la cataloga como alta, sin embargo, en urgencia de resolución tiene una puntuación de 9.7, por lo que se recomienda tomar medidas inmediatas debido a la protección que aporta ante malware peligroso basado en el exploits desarrollado por la NSA y filtrado por el grupo "Shadow Brokers": ETERNALBLUE. Para mitigar los efectos de estos códigos maliciosos, además de las actualizaciones de Microsoft, se recomienda, deshabilitar el SMBv1, segmentar la red para poder imponer medidas de contención y monitorizar la red.</p> <p>Aunque sea considerada de alta severidad, es crítica por la urgencia, debido a la amenaza de WannaCry al sistema.</p>
CVE-2017-0144	<u>(ETERNALBLUE)</u>	
CVE-2017-0143	<u>(ETERNALCHAMPION)</u>	
CVE-2017-0146	<u>(ETERNALROMANCE)</u>	
CVE-2017-0147	<u>(ETERNALSYNERGY)</u>	
CVE-2017-0148	<u>(WannaCry) (EternalRocks) (Petya) (uncredentialed check):</u>	
	<p>Presenta múltiples vulnerabilidades por ataque de divulgación de la información a través del protocolo SMB, además poder ser explotado por diversos Ransomware, destacando: WannaCry</p> <p>Como ejemplo de cómo sería la explotación con el exploit EternalBlue usando Python (imagen).</p>	
<pre> import socket # Libreria para la conexion de red import struct # Libreria para empaquetar datos en bytes # Dirección IP del objetivo target_ip = "192.168.1.100" target_port = 445 # Payload para ejecutar código arbitrario payload = b"\x90" * 100 # uso de NOP sled(No Operation sled(set de datos nulos)), para facilitar la explotación de la vulnerabilidad payload += b"\xcc" * 100 # uso de INT3 instructions (breakpoints) para detener el código y depurar #concatenando y multiplicando los valores de los bytes # Conexión al puerto SMB por el puerto 445 (TCP) s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)#creando un socket para la conexión s.connect((target_ip, target_port))#conectando al objetivo # Enviar el payload al objetivo s.send(payload) # Cerrar la conexión para liberar recursos s.close() print("Payload enviado. Verifica si el sistema objetivo ha sido comprometido.") </pre>		

INFORME TÉCNICO – RETO 4

<p>Nessus ID 35291</p> <p>CVE-2004- 2761</p> <p>CVE- 2005_4900</p>	<p><u>SSL Certificate Signed Using Weak Hashing Algorithm:</u> 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> Nessus considera SSL de resistencia media los cifrados que usen entre 64 a 112 bits o el 3DES.</p> <p>Como ejemplo de como se puede atacar con esta vulnerabilidad, vamos a imaginar un contexto donde el servidor web usa el certificado SSL firmado mediante un algoritmo MD5.</p> <p>1-Escaner de vulnerabilidades con Nessus: “nessus -q -x -T nessus_scan.xml -i nessus_scan.nessus”</p> <p>2-Generacion certificación falsa, usando técnicas de colisión (imagen1).</p> <p>3- Interceptación del tráfico con el certificado falso, realizando un ataque MITM, usando mitmproxy: “mitmproxy --certs fake_cert.pem”</p> <p>4-Acceso a la información sensible.</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 pública de certificados para que emita otro, ya que existen exploits públicos que pueden realizar estas acciones, explotando esta debilidad. Se recomienda el uso de cifrados de 128bit en adelante.</p> <p>Este plugin reporta todas las cadenas de certificados SSL firmadas con SHA-1 que expiran después del 1 de enero de 2017 como vulnerables, de acuerdo con el arreglo gradual de Google del algoritmo de hash criptográfico SHA-1.</p> <p>EL dispositivo objeto de este análisis, utiliza certificados SHA1 y MD5 por lo que es vulnerable, siendo aconsejable utilizar algoritmos mas seguros.</p>
	<pre> from hashlib import md5 # Certificado original obtenido con nessus o similar original_cert = b"Certificado original con MD5" original_hash = md5(original_cert).hexdigest() # Certificado falso usando tecnicas de colision, para generar un certificado falso con la misma firma digital fake_cert = b"Certificado falso con MD5" fake_hash = md5(fake_cert).hexdigest() # Verificación de colisión de hash MD5 if original_hash == fake_hash: print("Colisión exitosa: El certificado falso tiene la misma firma digital que el original.") else: print("No se pudo generar una colisión.") </pre>	

INFORME TÉCNICO – RETO 4

<p>Nessus ID 58435</p> <p>CVE-2012-0002</p> <p>CVE-2012-0152</p> <p>Se recomienda actualizar los parches publicados por Microsoft rápidamente, ya que, además, existen exploits públicos que pueden explotar esta vulnerabilidad, siendo el dispositivo objeto de análisis vulnerable:</p>	<p><u>MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (unauthenticated check):</u></p> <p>Ejecución de código por un atacante consistente en una secuencia de paquetes RDP especialmente diseñados al sistema afectado, 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. Esta vulnerabilidad podría ser explotada usando los programas Metasploit y Nmap de la forma siguiente:</p> <p>1-Escaner de vulnerabilidades del objetivo usando Nmap: <code>"nmap -p 3389 --script rdp-vuln-ms12-020 <IP_objetivo>"</code></p> <p>2- Configurar Metasploit, cargando el módulo específico para explotar esta vulnerabilidad.</p> <p>3-Configurar Metasploit con la IP_objetivo y el puerto y ejecutamos ataque.</p>	<p>Vulnerabilidad catalogada de alta severidad, pero el VPR de un 9.6, por lo que a efectos de urgente resolución es como si fuera crítica.</p> <p>Si el Protocolo de Escritorio Remoto (RDP) está habilitado en un sistema vulnerable, un atacante remoto no autenticado podría explotar esta vulnerabilidad, para ejecutar código arbitrario enviando paquetes RDP especialmente diseñados. Además, esta vulnerabilidad también permite ataques de denegación de servicio en Microsoft Terminal Server, sin embargo, el script de detección no identifica la vulnerabilidad si la opción de "Permitir solo conexiones desde computadoras que ejecutan Escritorio Remoto con Autenticación a nivel de red" está activada o si la capa de seguridad está configurada en "SSL (TLS 1.0)" en el host remoto.</p>
	<pre> --\$ nmap -p 3389 --script rdp-vuln-ms12-020 192.168.56.103 Starting Nmap 7.94SVN (https://nmap.org) at 2024-07-02 05:30 CEST Nmap scan report for 192.168.56.103 Host is up (0.00072s latency). PORT STATE SERVICE 3389/tcp open ms-wbt-server Nmap done: 1 IP address (1 host up) scanned in 62.29 seconds Metasploit Documentation: https://docs.metasploit.com/ msf6 > search ms12-020 Matching Modules ===== # Name Disclosure Date Rank Check Description - - 0 auxiliary/scanner/rdp/ms12_020_check 2012-03-16 normal Yes MS12-020 Microsoft Remote Desktop Checker 1 auxiliary/dos/windows/rdp/ms12_020_maxchannelids 2012-03-16 normal No MS12-020 Microsoft Remote Desktop Use-After-Free DoS Interact with a module by name or index. For example info 1, use 1 or use auxiliary/dos/windows/rdp/ms12_020_maxchannelids msf6 > use auxiliary/scanner/rdp/ms12_020_check msf6 auxiliary(scanner/rdp/ms12_020_check) > set RHOSTS 192.168.56.103 RHOSTS => 192.168.56.103 msf6 auxiliary(scanner/rdp/ms12_020_check) > run [+] 192.168.56.103:3389 - 192.168.56.103:3389 - The target is vulnerable. [*] 192.168.56.103:3389 - Scanned 1 of 1 hosts (100% complete) [*] Auxiliary module execution completed </pre>	

INFORME TÉCNICO – RETO 4

SEVERIDAD MEDIA				
Nessus ID 90510 CVE-2016-0128	<u>MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check):</u> El sistema Windows remoto tiene una vulnerabilidad que permite con un ataque MITM que un intruso pueda elevar sus privilegios debido a problemas en los protocolos de la Cuenta de Seguridad que contiene la base de datos donde Windows guarda la información sobre las cuentas de usuario y grupo, incluyendo contraseñas y políticas de seguridad (SAM) y la Autoridad de Seguridad Local donde se encuentra la base de datos que contiene información sobre políticas de seguridad, privilegios de usuario y otros datos relacionados con la seguridad del sistema, usando el canal LSAD para acceder (LSA). Esta vulnerabilidad se debe a una negociación inadecuada del nivel de autenticación en los canales de Llamada de Procedimiento Remoto (RPC). Un atacante que pueda interceptar las comunicaciones entre un cliente y un servidor que maneja una base de datos SAM puede aprovechar esta vulnerabilidad para reducir el nivel de autenticación, lo que le permitiría hacerse pasar por un usuario autenticado y acceder a la base de datos SAM.		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, pero pueden ser explotados con herramientas específicas. Además de las actualizaciones, es recomendable para mitigar efectos, configurar la NLA como habilitada (autenticación a nivel de red), configurar el servicio RDP para usarlo con SSL/TLS y deshabilitar el RDP si no es necesario. El dispositivo objeto de estudio se ha comprobado que es vulnerable, como se muestra en la imagen que tiene una única actualización y no es para esta vulnerabilidad, la cual sería esta MS16-047 (KB3140410)	
				

INFORME TÉCNICO – RETO 4

Nessus ID 58751	<u>SSL/TLS Protocol Initialization</u> <u>Vector Implementation</u> <u>Information Disclosure</u> <u>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 de manera técnica un total de 16 vulnerabilidades reales, habiendo descartado las vulnerabilidades en que los dispositivos no son vulnerables por diversas causas favorables:

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

5.- Conclusiones

En este informe se han detallado las formas de cómo se pueden explotar algunas de las vulnerabilidades en los sistemas objeto de estudio, 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 toda su empresa.

INFORME TÉCNICO – RETO 4

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>

INFORME TÉCNICO – RETO 4

--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>