



EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA



TECNOLÓGICO
NACIONAL DE MÉXICO®



INSTITUTO TECNOLÓGICO DE MORELIA
"José María Morelos y Pavón"

INSTITUTO TECNOLÓGICO DE MORELIA

Ingeniería en Sistemas Computacionales

Hardening de Servidores

Práctica 2

ALUMNO:

Rogelio Cristian Punzo Castro

PROFESOR:

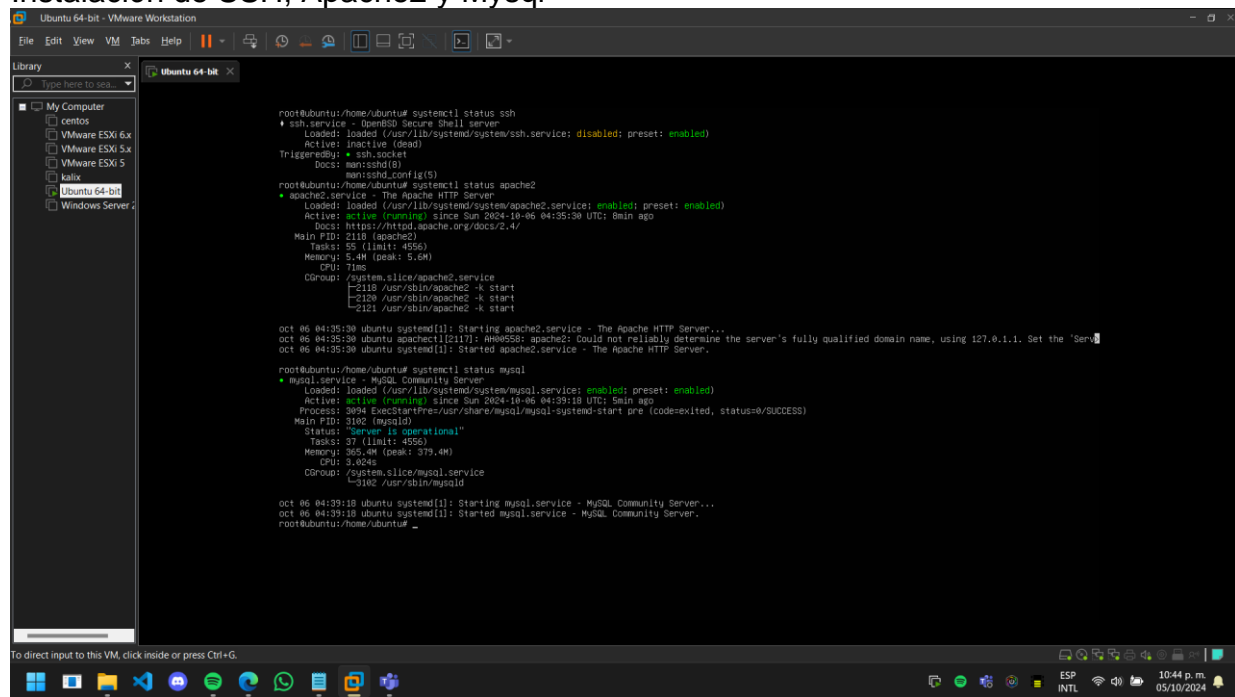
Juan Jesús Ruiz Lagunas

MORELIA, MICHOACÁN

(Octubre 2024)

Linux (Ubuntu)

Instalación de SSH, Apache2 y Mysql



```
root@ubuntu:/home/ubuntu# systemctl status ssh
* ssh.service - OpenSSH Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
   Active: inactive (dead)
   TriggeredBy: * ssh.socket
   Docs: man:sshd(8)
         man:sshd_config(5)

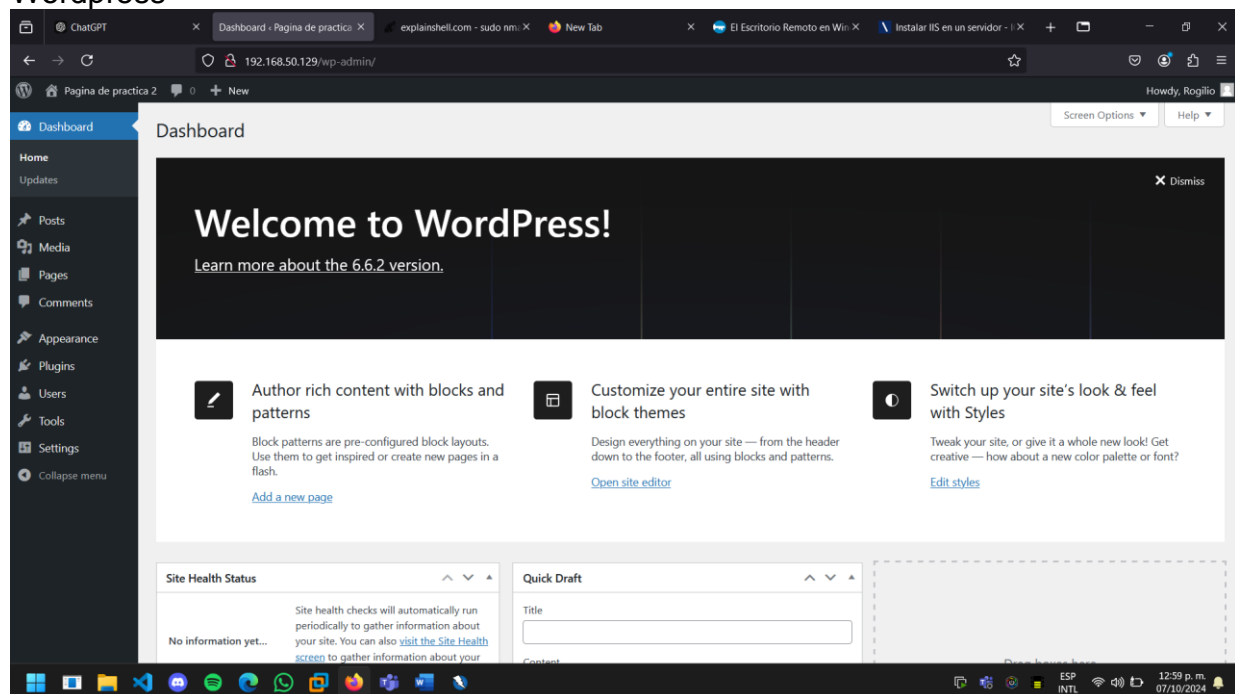
root@ubuntu:/home/ubuntu# systemctl status apache2
* apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Sun 2024-10-06 04:35:30 UTC; 8min ago
   Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2118 (apache2)
   Tasks: 55 (limit: 4556)
   Memory: 5.4M (peak: 5.6M)
   CPU: 71ms
   CGroup: /system.slice/apache2.service
           └─2118 /usr/sbin/apache2 -k start
           └─2120 /usr/sbin/apache2 -k start
           └─2121 /usr/sbin/apache2 -k start

oct 06 04:35:30 ubuntu systemd[1]: Starting apache2.service - The Apache HTTP Server...
oct 06 04:35:30 ubuntu apachectl[2117]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1. Set the 'ServerName' directive dynamically to determine the server's name.
oct 06 04:35:30 ubuntu systemd[1]: Started apache2.service - The Apache HTTP Server.

root@ubuntu:/home/ubuntu# systemctl status mysql
* mysql.service - MySQL Community Server
   Loaded: loaded (/usr/lib/systemd/system/mysql.service; enabled; preset: enabled)
   Active: active (running) since Sun 2024-10-06 04:39:18 UTC; 5min ago
   Process: 3054 ExecStartPre=/usr/share/mysql/mysql-systemd-start pre (code=exited, status=0/SUCCESS)
   Main PID: 3102 (mysqld)
   Status: "Server is operational"
   Tasks: 37 (limit: 4556)
   Memory: 365.4M (peak: 379.4M)
   CPU: 3.624s
   CGroup: /system.slice/mysql.service
           └─3102 /usr/sbin/mysqld

oct 06 04:39:18 ubuntu systemd[1]: Starting mysql.service - MySQL Community Server...
oct 06 04:39:18 ubuntu systemd[1]: Started mysql.service - MySQL Community Server.
root@ubuntu:/home/ubuntu#
```

Wordpress



1. Falta de la cabecera X-Frame-Options

- **Descripción:** Esta cabecera HTTP es utilizada para proteger contra ataques de clickjacking. La ausencia de esta cabecera permite que otros sitios web puedan cargar tu contenido en un <iframe> dentro de su página, lo que podría ser explotado por un atacante para engañar a los

usuarios y hacer que realicen acciones indeseadas (como clics o envío de formularios).

- **Impacto:** Permite ataques de clickjacking, que pueden llevar a la ejecución involuntaria de acciones por parte del usuario autenticado. En el peor de los casos, se pueden robar credenciales o realizar acciones en el sitio en nombre del usuario.
- **Recomendación:** Configurar la cabecera X-Frame-Options en el servidor con uno de los siguientes valores:
 - DENY: Bloquea la inclusión del contenido en cualquier iframe.
 - SAMEORIGIN: Permite la inclusión solo si el contenido proviene del mismo origen.

2. Falta de la cabecera X-Content-Type-Options

- **Descripción:** La cabecera X-Content-Type-Options con el valor nosniff previene que los navegadores interpreten el contenido de forma diferente a su tipo MIME declarado. Sin esta cabecera, un atacante podría inyectar scripts en archivos que normalmente no serían considerados ejecutables.
- **Impacto:** Un atacante podría forzar la interpretación incorrecta de tipos de archivos, lo cual puede ser explotado para ataques XSS (Cross-Site Scripting). Esto comprometería la integridad de la aplicación y la información de los usuarios.
- **Recomendación:** Agregar la cabecera X-Content-Type-Options: nosniff a las respuestas HTTP para evitar que el navegador interprete incorrectamente el tipo de contenido.

3. Cabecera no común 'x-redirect-by' con contenido 'WordPress'

- **Descripción:** La presencia de la cabecera x-redirect-by en las respuestas HTTP indica que el servidor utiliza WordPress, lo cual facilita a los atacantes la identificación del CMS y la búsqueda de vulnerabilidades conocidas de WordPress.
- **Impacto:** La identificación del CMS y de plugins específicos permite a los atacantes enfocar sus esfuerzos en explotar vulnerabilidades conocidas de la versión de WordPress o de los plugins utilizados.
- **Recomendación:** Deshabilitar el uso de esta cabecera a través de la configuración del servidor o mediante plugins de seguridad de WordPress para reducir la exposición de información innecesaria.

4. Posible fuga de información a través de ETags

- **Descripción:** Las cabeceras ETag pueden revelar detalles internos del servidor, como el uso de inodos, que son identificadores de archivos en el sistema de archivos. Esto podría ayudar a un atacante a mapear el sistema de archivos del servidor.
- **Impacto:** Un atacante puede usar esta información para realizar ataques de sincronización de caché o correlacionar recursos entre diferentes servidores, ayudando a detectar configuraciones incorrectas o estructuras internas del servidor.
- **Recomendación:** Deshabilitar el uso de ETags configurando el servidor Apache para que no las incluya en las respuestas, mediante FileETag None.

5. Métodos HTTP Permitidos: OPTIONS, HEAD, GET, POST

- **Descripción:** Los métodos HTTP permiten a los clientes interactuar con el servidor de diversas formas. Sin embargo, no todos los métodos son necesarios para el funcionamiento de una aplicación web estándar.
- **Impacto:** Permitir métodos como OPTIONS puede facilitar a los atacantes mapear las capacidades del servidor, lo cual podría llevar a la explotación de funcionalidades no seguras.
- **Recomendación:** Restringir los métodos HTTP a solo aquellos necesarios para la aplicación (generalmente GET y POST) mediante la configuración de seguridad del servidor Apache.

6. Output de phpinfo() disponible

- **Descripción:** La página info.php revela información detallada sobre la configuración de PHP, incluyendo módulos habilitados, variables de entorno y rutas de directorios. Esta información puede ser valiosa para un atacante.
- **Impacto:** Los atacantes pueden usar esta información para identificar posibles vectores de ataque específicos del entorno PHP, como módulos vulnerables o configuraciones inseguras.
- **Recomendación:** Eliminar la página info.php del servidor o, si es necesaria para el diagnóstico, restringir su acceso con autenticación.

7. Inyección de Archivos Remotos (RFI)

- **Descripción:** Se detectó la vulnerabilidad de inclusión de archivos remotos (RFI) en un script que permite incluir archivos externos. Esto puede permitir que un atacante cargue y ejecute código malicioso desde un servidor remoto.
- **Impacto:** Los ataques RFI pueden resultar en la ejecución de comandos arbitrarios, instalación de backdoors, y control total del servidor comprometido.
- **Recomendación:**
 - Validar y sanitizar todas las entradas de usuario.
 - Deshabilitar allow_url_include en la configuración de PHP.
 - Implementar una lista blanca de archivos permitidos.

8. Cookie sin la bandera HttpOnly

- **Descripción:** Las cookies sin esta bandera pueden ser accedidas por scripts en el navegador.
- **Impacto:** Aumenta el riesgo de ataques XSS (Cross-Site Scripting).

9. Información del plugin Akismet y versión de WordPress

- **Descripción:** El archivo readme.txt de plugins como Akismet puede revelar la versión del plugin y, a menudo, la versión de WordPress. Esto facilita la identificación de vulnerabilidades específicas de la versión.
- **Impacto:** Conocer la versión de WordPress y de sus plugins puede permitir a un atacante realizar un ataque dirigido utilizando exploits conocidos para esas versiones.
- **Recomendación:** Eliminar archivos innecesarios que puedan exponer información de versiones, especialmente aquellos como readme.txt.

10. Indexación de Directorios en /wp-content/uploads/

- **Descripción:** El acceso a la estructura de archivos del directorio de subidas de WordPress permite que cualquier usuario vea los archivos almacenados, lo cual podría incluir documentos sensibles o imágenes privadas.
- **Impacto:** La exposición de archivos puede revelar información confidencial o ayudar a un atacante a identificar la estructura de la aplicación y los tipos de archivos disponibles.
- **Recomendación:** Deshabilitar la indexación de directorios mediante un archivo .htaccess con la directiva Options -Indexes.

11. Cookie wordpress_test_cookie sin la flag HttpOnly

- **Descripción:** Las cookies sin la flag HttpOnly pueden ser accedidas desde scripts JavaScript, lo cual incrementa el riesgo de ser explotadas mediante XSS.
- **Impacto:** Un ataque XSS podría permitir a un atacante robar cookies de sesión, lo que podría dar acceso a la cuenta del usuario autenticado.
- **Recomendación:** Configurar las cookies de WordPress para que tengan la flag HttpOnly y Secure (para HTTPS).

12. CVE-2024-6387:

- **Severidad:** 8.1 (Alta)
- **Descripción:** Una vulnerabilidad de ejecución remota de código (RCE) que afecta a OpenSSH 9.6p1, permitiendo a un atacante ejecutar comandos en el sistema afectado. Esto puede comprometer por completo la máquina si el atacante obtiene acceso privilegiado.
- **Impacto:** Permite a atacantes remotos ejecutar comandos arbitrarios en el sistema, comprometiendo la integridad y confidencialidad del servidor.
- **Exploit:** [Enlace al exploit](#)

13. Exploit 95499236-C9FE-56A6-9D7D-E943A24B633A:

- **Severidad:** 10.0 (Crítica)
- **Descripción:** Vulnerabilidad crítica que permite la explotación a través de un vector de ataque remoto, aprovechando una mala configuración o defecto en la implementación de OpenSSH.
- **Impacto:** Puede permitir a un atacante la ejecución de código remoto con privilegios elevados.
- **Exploit:** [Enlace al exploit](#)

14. Exploit 2C119FFA-ECE0-5E14-A4A4-354A2C38071A:

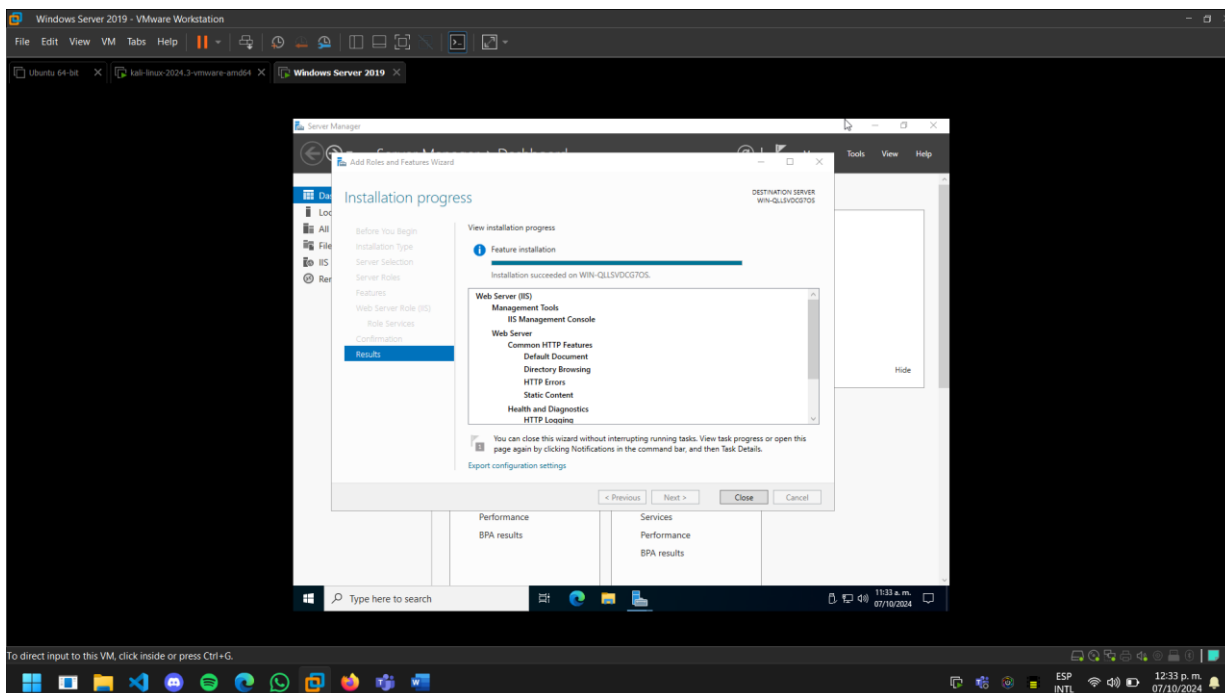
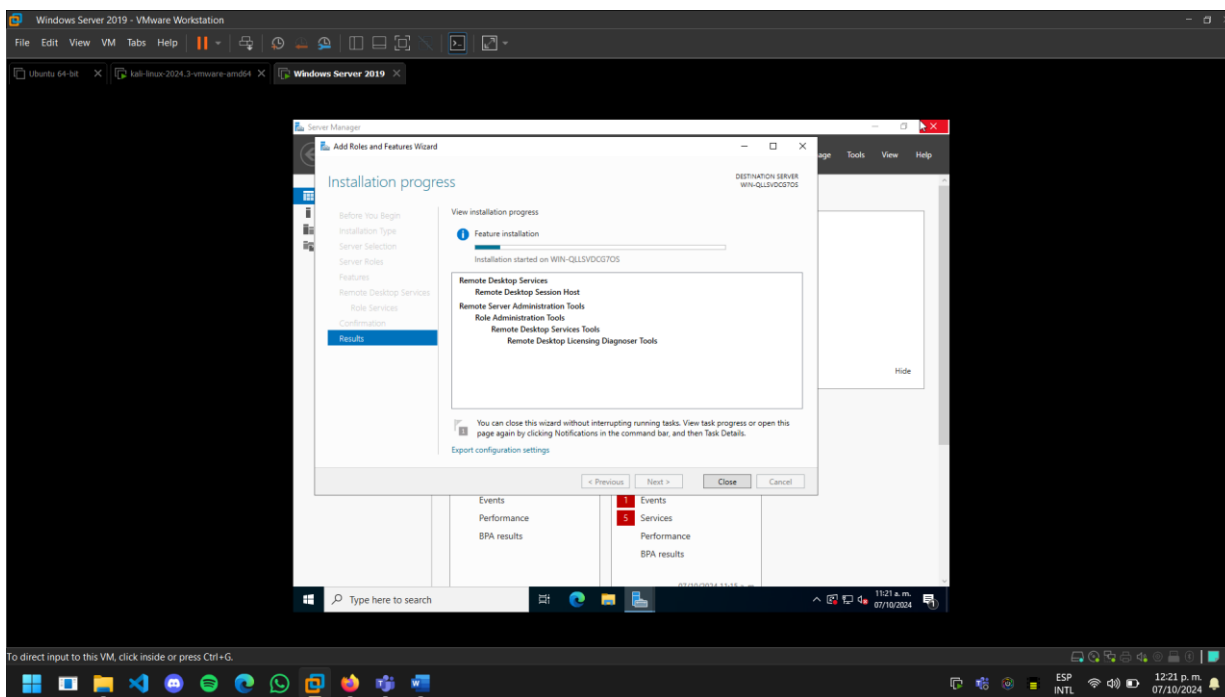
- **Severidad:** 10.0 (Crítica)
- **Descripción:** Exploit que aprovecha un desbordamiento de búfer en el servicio OpenSSH, lo cual puede ser utilizado para obtener acceso administrativo.
- **Impacto:** La explotación exitosa permite un control total del sistema afectado.
- **Exploit:** [Enlace al exploit](#)

15. Exploit 5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A:

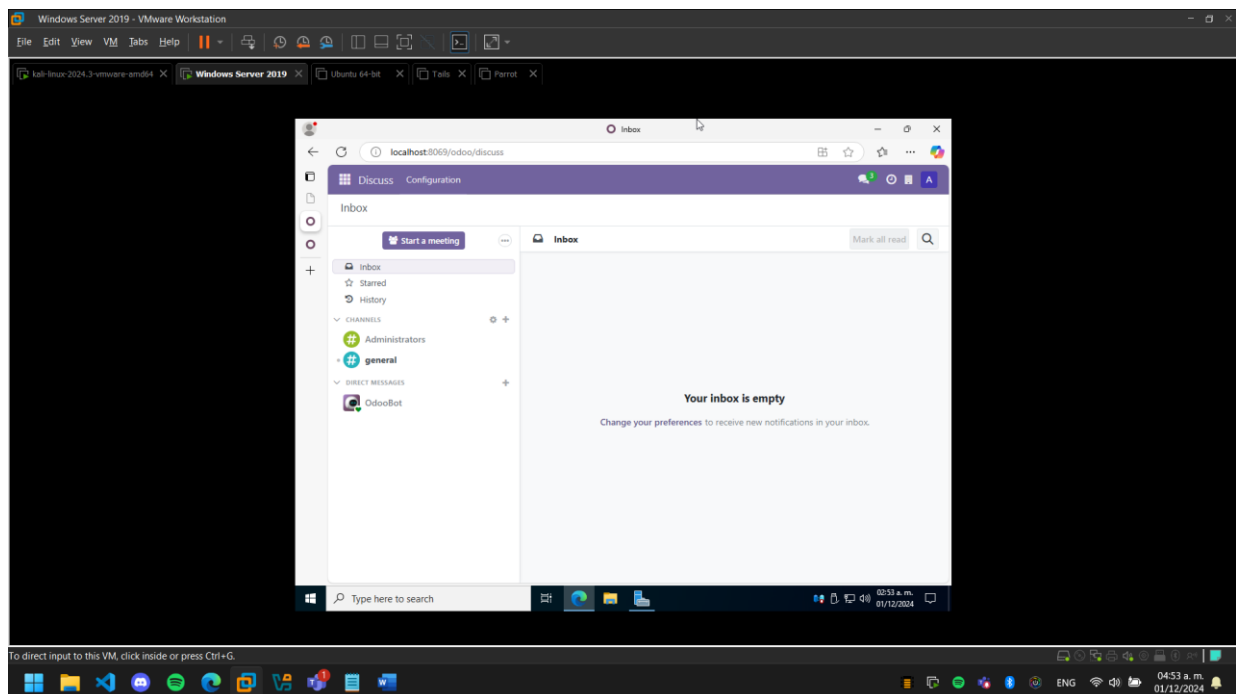
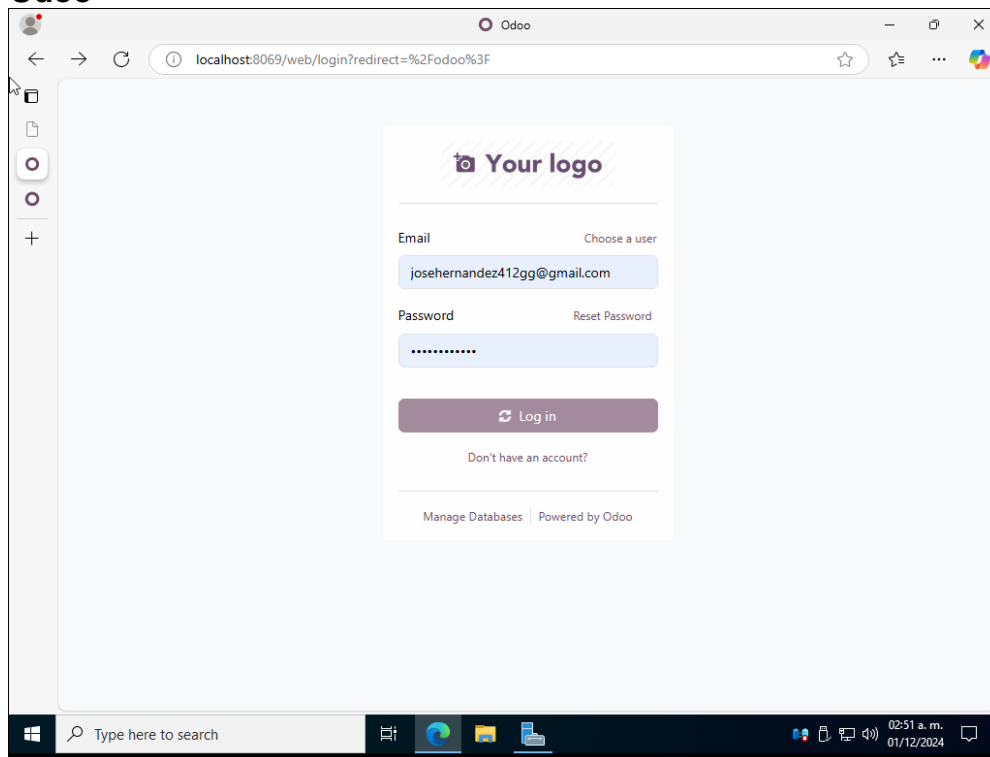
- **Severidad:** 9.8 (Alta)

- **Descripción:** Una vulnerabilidad de tipo RCE en OpenSSH que permite a un atacante ejecutar código en el servidor mediante una petición maliciosa.
 - **Impacto:** Riesgo alto de pérdida de control del sistema y acceso no autorizado a datos sensibles.
 - **Exploit:** [Enlace al exploit](#)
16. **Exploit PACKETSTORM:179290:**
- **Severidad:** 8.1 (Alta)
 - **Descripción:** Exploit que aprovecha una vulnerabilidad en la implementación de OpenSSH para realizar ataques de fuerza bruta o evadir autenticación.
 - **Impacto:** Posibilidad de acceder al sistema sin necesidad de credenciales válidas, exponiendo el sistema a riesgos de pérdida de información.
 - **Exploit:** [Enlace al exploit](#)

Windows Server



Odoo





- **Servicio:** IIS (Internet Information Services) 10.0.
- **Descripción:** Esta cabecera HTTP previene que el contenido de la página se muestre dentro de un iframe, protegiendo contra ataques de "clickjacking". Al no estar presente, una página maliciosa podría superponer un iframe de la página legítima para engañar al usuario y que realice acciones indeseadas sin darse cuenta.
- **Funcionalidad de la Vulnerabilidad:** Permite que una página web se incruste dentro de un iframe en un dominio diferente, lo que hace que un atacante pueda engañar a los usuarios para que realicen acciones no deseadas en su sitio mientras creen estar interactuando con el sitio legítimo.
- **Impacto:** Riesgo de ataques de clickjacking, que podría llevar a la pérdida de control sobre la cuenta del usuario o la ejecución de acciones no autorizadas.

- **Servicio:** IIS 10.0.
- **Descripción:** Esta cabecera le dice al navegador que no debe cambiar el tipo MIME del contenido recibido, evitando así la ejecución de scripts que podrían ser maliciosos en archivos que no se esperaba ejecutar. Sin esta cabecera, es posible que un atacante logre ejecutar código al hacer que el navegador interprete archivos de manera incorrecta.
- **Funcionalidad de la Vulnerabilidad:** El navegador puede "adivinar" el tipo de contenido de un archivo en lugar de seguir el tipo MIME

especificado por el servidor, lo que podría llevar a la ejecución de contenido no deseado.

- **Impacto:** Riesgo de ataques de "MIME Sniffing", donde los archivos de tipo incorrecto podrían ejecutarse y comprometer la seguridad de la aplicación web o del servidor.

3. **Métodos HTTP Permitidos: OPTIONS, TRACE, GET, HEAD, POST**

- **Servicio:** IIS 10.0.
- **Descripción:** La disponibilidad de métodos como OPTIONS y TRACE puede ser problemática. TRACE, por ejemplo, puede ser usado en ataques de tipo "Cross-Site Tracing (XST)" para capturar cookies de autenticación y otra información sensible. Aunque el método GET y POST son necesarios para la funcionalidad de la mayoría de las aplicaciones web, la exposición de TRACE y OPTIONS debe ser controlada.
- **Funcionalidad de la Vulnerabilidad:** El método TRACE puede ser usado para realizar un ataque de XST, donde un atacante envía una solicitud TRACE a la aplicación y esta devuelve la información de la cabecera de la solicitud. Esto puede incluir cookies de autenticación o encabezados sensibles.
- **Impacto:** Riesgo de XST y exposición de información del servidor que podría ser útil para un atacante al mapear la aplicación web.

Puertos y Servicios Abiertos

1. **80/tcp - HTTP:**

- Servidor: Microsoft IIS 10.0
- Información adicional:
 - Métodos HTTP potencialmente riesgosos: TRACE.
 - Posibles problemas de configuración de seguridad, como cabeceras de seguridad HTTP no configuradas adecuadamente.
- Vulnerabilidad potencial: Puede permitir ataques XSS o CSRF si no se configura correctamente.

2. **135/tcp - msrpc:**

- Protocolo Microsoft RPC, típico en sistemas Windows para servicios remotos.
- Vulnerabilidad potencial: Puede ser explotado para el acceso remoto o para ejecutar comandos arbitrarios si no está adecuadamente protegido.

3. **445/tcp - microsoft-ds (SMB):**

- Protocolo SMB, comúnmente utilizado para compartir archivos en red.
- Información adicional:
 - Compatible con varias versiones de SMB, incluyendo SMBv3.
 - Firma de mensajes habilitada pero no requerida.
- Vulnerabilidad potencial: SMB ha sido objetivo de exploits como EternalBlue, lo que podría permitir la ejecución remota de código si el sistema no está parcheado.

4. **3389/tcp - Microsoft Terminal Services (RDP):**

- Servicio de Escritorio Remoto.
- Seguridad habilitada: CredSSP (NLA).

- Vulnerabilidad potencial: RDP es un objetivo común de ataques de fuerza bruta. Si no se protege adecuadamente (NLA, autenticación de dos factores), puede comprometerse.

5. **5357/tcp - Microsoft HTTPAPI (SSDP/UPnP):**

- Servidor HTTPAPI de Microsoft, generalmente utilizado para SSDP/UPnP.
- Estado: Servicio no disponible.
- Vulnerabilidad potencial: UPnP puede ser utilizado para ataques de red internos si está mal configurado.

Hallazgos Adicionales

- **Posible Fuga de Información:**

- Existen comentarios HTML en la página principal del servidor IIS (puerto 80).
- El escaneo de nmap sugiere que algunos scripts no pueden extraer datos debido a cambios en APIs externas (como Robtex).

- **Configuración de Red:**

- La máquina responde a solicitudes de multicast y descubrimiento de DHCP.
- Información DHCP sugiere que el rango de red es 192.168.50.x, con una máscara de subred de 255.255.255.0.