

CIBER SEGURIDAD PROYECTO FINAL

SEARCH icon ALEJANDRO GIL SÁNCHEZ SPEECH icon



MAYO 2025





HERRAMIENTAS UTILIZADAS



Nmap

Herramienta de código abierto que se utiliza para mapear redes y realizar análisis de seguridad.



Netcat

Herramienta de back-end que permite el escaneo y la escucha de puertos



Hydra

Software enfocado al hacking para ejecutar ataques de fuerza bruta.



INTRUSIÓN EN SERVIDOR PRINCIPAL



Cuando entra el atacante

Identificamos la fecha y hora:

- 8 de octubre
- 17:40:59



IP del atacante

- 192.168.0.134
- Misma subred que la de la víctima



Vector de entrada

- SSH (acceso no autorizado)
- Credenciales débiles o comprometidas



Actividades maliciosas detectadas

- Modificación de permisos /var/www/html
- Cambio de direcciones IPv4 e IPv6
- Creación de usuario "user" en MySQL con todos los privilegios





NUEVAS VULNERABILIDADES DETECTADAS



FTP Anonymous

Acceso anónimo habilitado, cualquiera se puede conectar poniendo como nombre: anonymous

FTP - DDoS

La versión vsFTPD 3.0.3 permite hacer peticiones masivas al FTP sin limitaciones

HTTP - Wordpress

Se puede listar/enumarar los directorios o archivos de wordpress y acceder a información o rutas interesantes.





EXPLORACIÓN WORDPRESS



ENUMERACIÓN DE DIRECTORIOS

Herramienta



Gracias a esta herramienta enumeraremos directorios y archivos ocultos.

Descubrimientos

Logramos acceder a rutas y archivos sensibles como:

- wp-includes : contiene librerías centrales de Wordpress
- wp-content/uploads: almacena archivos subidos por usuarios.

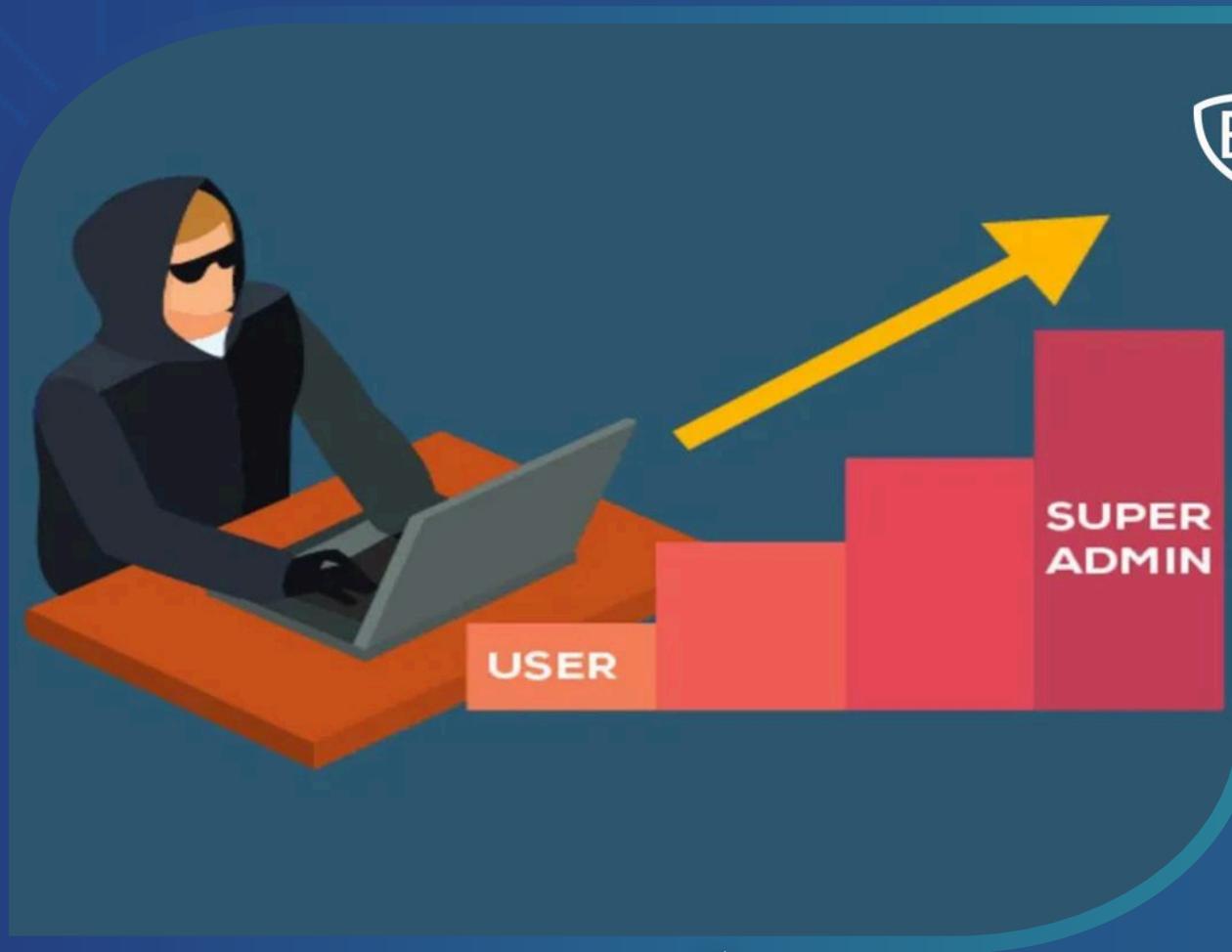
| Name | Last modified | Size | Description |
|--------------------------|------------------|------|-------------|
| Parent Directory | | - | |
| ID3/ | 2024-09-10 11:23 | - | |
| IXR/ | 2024-09-10 11:23 | - | |
| PHPMailer/ | 2024-09-10 11:23 | - | |
| Requests/ | 2024-09-10 11:23 | - | |
| SimplePie/ | 2025-05-10 13:21 | - | |
| Text/ | 2025-05-10 13:21 | - | |
| admin-bar.php | 2025-05-10 13:21 | 36K | |
| assets/ | 2025-05-10 13:21 | - | |
| atomb.php | 2025-05-10 13:21 | 12K | |
| author-template.php | 2023-05-14 13:58 | 19K | |
| block-bindings.php | 2024-06-12 08:44 | 5.5K | |
| block-bindings/ | 2024-09-10 11:23 | - | |
| block-editor.php | 2025-05-10 13:21 | 28K | |
| block-i18n.json | 2021-08-11 05:08 | 316 | |
| block-patterns.php | 2025-05-10 13:21 | 13K | |
| block-patterns/ | 2024-09-10 11:23 | - | |
| block-supports/ | 2025-05-10 13:21 | - | |
| block-template-utils.php | 2025-05-10 13:21 | 60K | |

| Name | Last modified | Size | Description |
|------------------|------------------|------|-------------|
| Parent Directory | | - | |
| 2024/ | 2024-10-08 16:49 | - | |
| 2025/ | 2025-05-20 08:05 | - | |





EXPLORACIÓN FTP



ESCALACIÓN DE PRIVILEGIOS

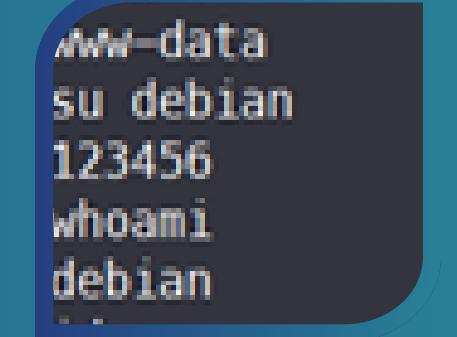
Ataque DoS - hping3

Con esta herramienta inundamos el Servidor de peticiones SYN hasta saturar el sistema.



Ataque de Fuerza Bruta - hydra

Sabiendo que FTP permite número ilimitado de peticiones, realizamos un Ataque de Fuerza Bruta.



Obtención de credenciales

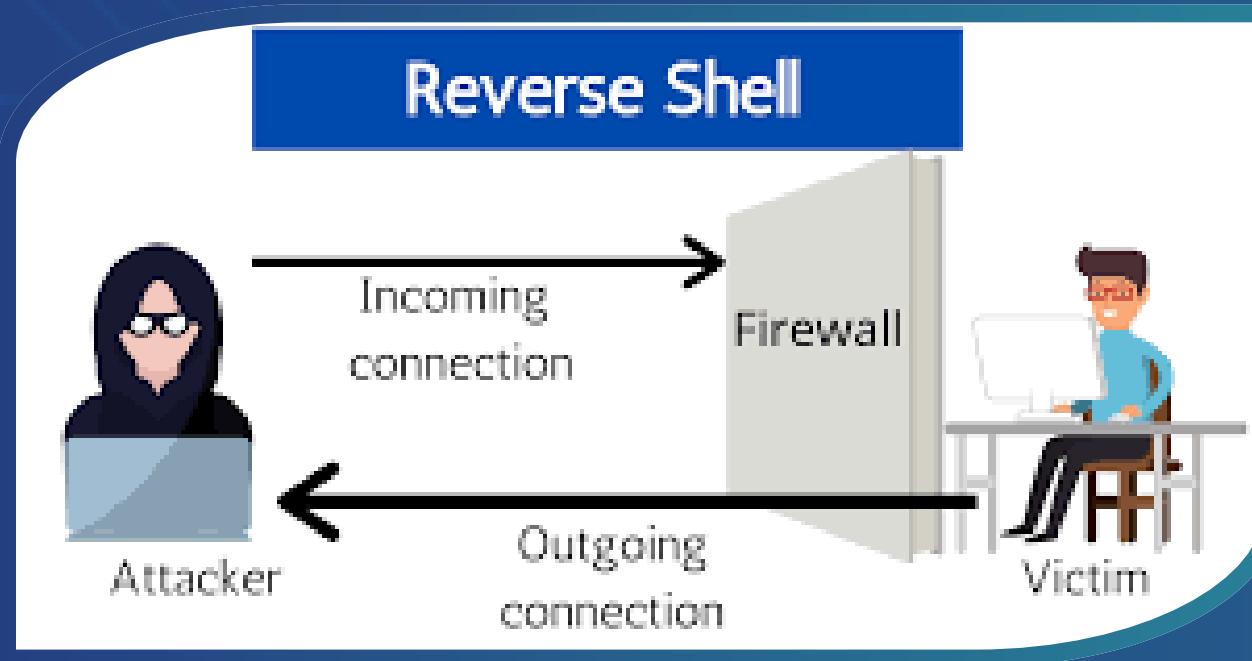
Obteniendo credenciales del usuario **"debian:123456"**.

De modo que hemos conseguido la escalación de privilegios ya que este usuario puede ejecutar sudo.





EXPLORACIÓN FTP



CREACIÓN REVERSE SHELL

Subida de archivos maliciosos.

Creamos un script en php para crear una reverse shell y lo subimos a wp-content/uploads.

| Index of /wp-content/uploads/ | | | |
|-------------------------------|------------------|------|-------------|
| Name | Last modified | Size | Description |
| Parent Directory | | - | |
| 2024/ | 2024-10-08 16:49 | - | |
| 2025/ | 2025-06-02 14:58 | - | |
| update_media.php | 2025-06-04 13:18 | 31 | |

Apache/2.4.62 (Debian) Server at 192.168.1.150 Port 80

Conexión Reverse Shell

Desde la Máquina Atacante, teniendo un puerto en modo escucha, introducimos la ruta deseada más un comando para establecer la reverse Shell.

Creación de usuario con privilegios

Para asegurarnos futuras conexiones y no depender de las credenciales de debian, además asignamos un nombre que pase desapercibido "**svc-media**"





Mitigaciones Genéricas



Es muy importante mantener cualquier sistema o servicio actualizado.



Cambiar contraseñas débiles por complejas y robustas:

- Mínimo 12 caracteres
- Mayúsculas, minúsculas y números.
- Caracteres especiales
- No repetir la misma contraseña.



Incluir herramientas de detección y respuesta a amenazas. Con el objetivo de monitorear todo lo que pasa en el sistema y tener un plan de acción en caso de incidente.

CONFIGURACIONES DE SEGURIDAD

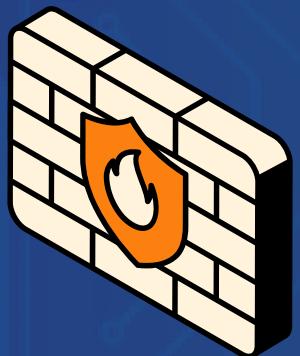




Mitigaciones Específicas



- Contraseñas seguras
- Autenticación Multifactor (MFA)



Configuración de Firewall (iptables):

- Restricción de número conexiones (FTP - SSH)
- Restricción de número de intentos al autenticarse
- Restringir acceso solo a IP autorizadas



Configuraciones más seguras:

- SSH - Prohibir acceso root, Autenticación por claves
- FTP - Deshabilitar acceso anónimo
- HTTP - reasignación de permisos
- MySQL - Eliminar usuario "user", mejorar credenciales

CONFIGURACIONES DE SEGURIDAD



THANK YOU!



Hrimthur



Alejandro Gil