Seguridad de Sistemas Informáticos.

Omar Teixeira González,
UO281847

Examen Práctico

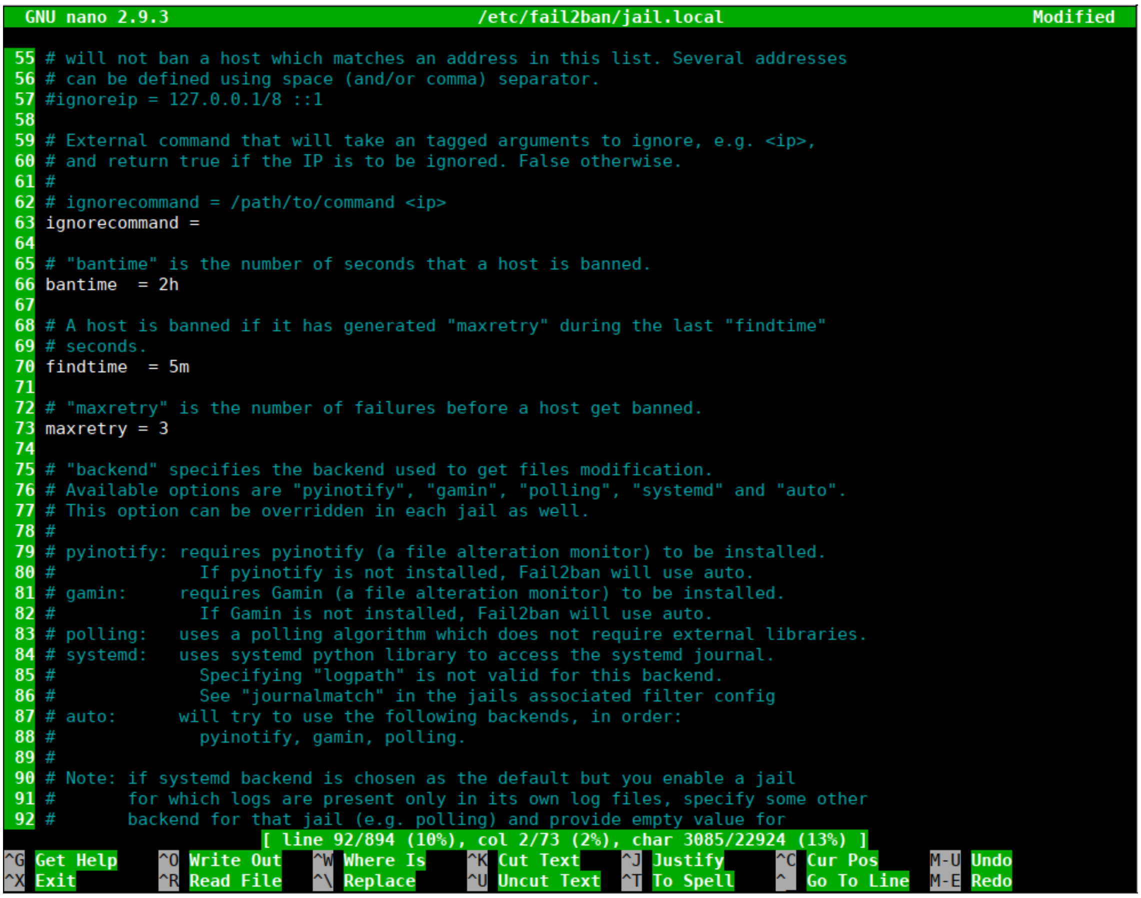
Tabla de contenidos

Ejercicio 1.

Para realizar este ejercicio se utiliza fail2ban, para ello (como el fichero jail.local no existe, se copia el jail.conf previamente), mediante *cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local* y se accede a este fichero para configurar las opciones.

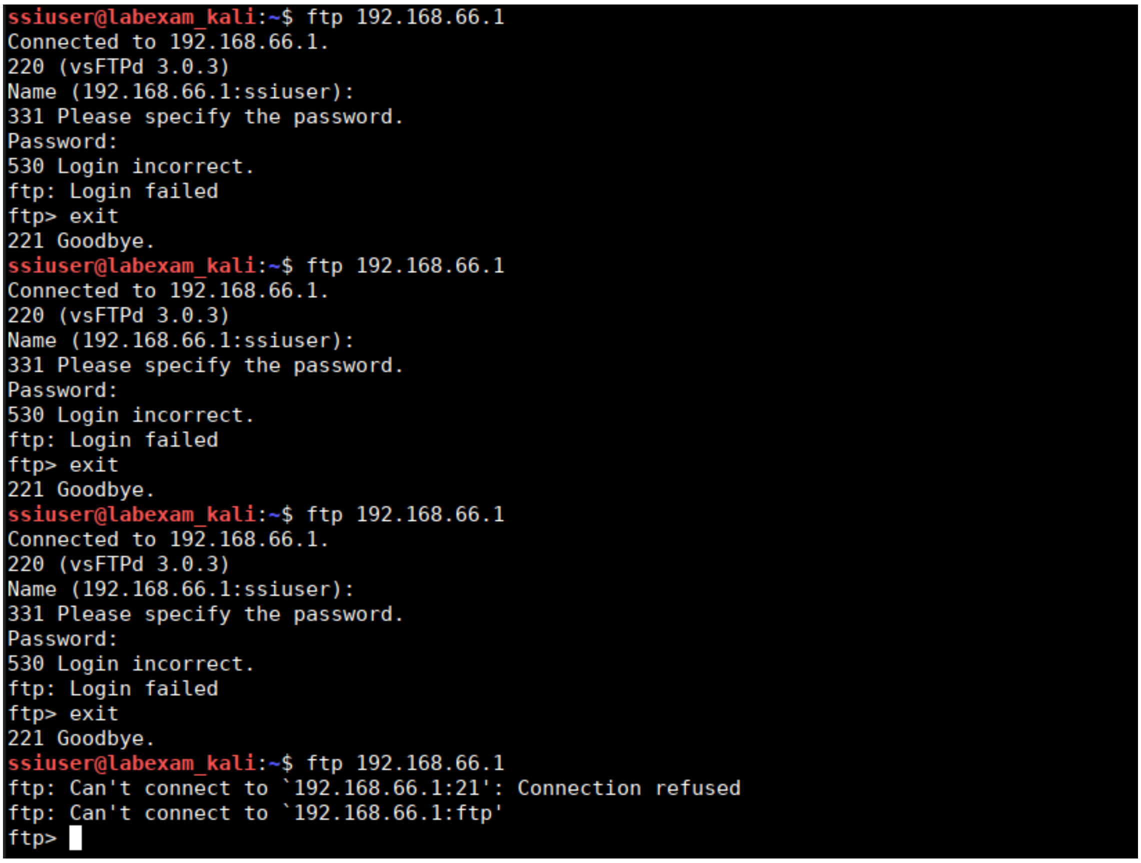
a. Modificaciones al fichero jail.local:

```
  GNU nano 2.9.3                          /etc/fail2ban/jail.local

492 port     = ftp,ftp-data,ftps,ftps-data
493 logpath  = %(pureftpd_log)s
494 backend  = %(pureftpd_backend)s
495
496
497 [gssftpd]
498
499 port     = ftp,ftp-data,ftps,ftps-data
500 logpath  = %(syslog_daemon)s
501 backend  = %(syslog_backend)s
502
503
504 [wuftpd]
505
506 port     = ftp,ftp-data,ftps,ftps-data
507 logpath  = %(wuftpd_log)s
508 backend  = %(wuftpd_backend)s
509
510
511 [vsftpd]
512 enabled = true
513 # or overwrite it in jails.local to be
514 # logpath = %(syslog_authpriv)s
515 # if you want to rely on PAM failed login attempts
516 # vsftpd's failregex should match both of those formats
517 port     = ftp,ftp-data,ftps,ftps-data
518 logpath  = %(vsftpd_log)s
519
520
521 #
522 # Mail servers
523 #
524
525 # ASSP SMTP Proxy Jail
526 [assp]
527
528 port     = smtp,465,submission
529 logpath  = /root/path/to/assp/logs/maillog.txt
                                        [ Wrote 891 lines ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line  M-E Redo
```



```
  GNU nano 2.9.3                  /etc/fail2ban/jail.local                  Modified

# will not ban a host which matches an address in this list. Several addresses
# can be defined using space (and/or comma) separator.
#ignoreip = 127.0.0.1/8 ::1

# External command that will take an tagged arguments to ignore, e.g. <ip>,
# and return true if the IP is to be ignored. False otherwise.
#
# ignorecommand = /path/to/command <ip>
ignorecommand =

# "bantime" is the number of seconds that a host is banned.
bantime  = 2h

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime  = 5m

# "maxretry" is the number of failures before a host get banned.
maxretry = 3

# "backend" specifies the backend used to get files modification.
# Available options are "pyinotify", "gamin", "polling", "systemd" and "auto".
# This option can be overridden in each jail as well.
#
# pyinotify: requires pyinotify (a file alteration monitor) to be installed.
#              If pyinotify is not installed, Fail2ban will use auto.
# gamin:     requires Gamin (a file alteration monitor) to be installed.
#              If Gamin is not installed, Fail2ban will use auto.
# polling:   uses a polling algorithm which does not require external libraries.
# systemd:   uses systemd python library to access the systemd journal.
#              Specifying "logpath" is not valid for this backend.
#              See "journalmatch" in the jails associated filter config
# auto:      will try to use the following backends, in order:
#              pyinotify, gamin, polling.
#
# Note: if systemd backend is chosen as the default but you enable a jail
#       for which logs are present only in its own log files, specify some other
#       backend for that jail (e.g. polling) and provide empty value for
                    [ line 92/894 (10%), col 2/73 (2%), char 3085/22924 (13%) ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line  M-E Redo
```

b. Tras intentar acceder 3 veces, se ha bloqueado:



```
ssiuser@labexam_kali:~$ ftp 192.168.66.1
Connected to 192.168.66.1.
220 (vsFTPd 3.0.3)
Name (192.168.66.1:ssiuser):
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> exit
221 Goodbye.
ssiuser@labexam_kali:~$ ftp 192.168.66.1
Connected to 192.168.66.1.
220 (vsFTPd 3.0.3)
Name (192.168.66.1:ssiuser):
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> exit
221 Goodbye.
ssiuser@labexam_kali:~$ ftp 192.168.66.1
Connected to 192.168.66.1.
220 (vsFTPd 3.0.3)
Name (192.168.66.1:ssiuser):
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> exit
221 Goodbye.
ssiuser@labexam_kali:~$ ftp 192.168.66.1
ftp: Can't connect to `192.168.66.1:21': Connection refused
ftp: Can't connect to `192.168.66.1:ftp'
ftp> 
```

c. Usando el comando *fail2ban-client status vsftpd*, se comprueba que la ip se ha bloqueado:

```
ssiuser@vagrant:~/Desktop/ssi_labs/lab_exam$ sudo fail2ban-client status vsftpd
Status for the jail: vsftpd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     10
|  `- File list:        /var/log/vsftpd.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.66.6
```

d. Se desbloquea la ip con *fail2ban-client set vsftpd unbanip 192.168.66.6*, y se comprueba el estado de bloqueo:

```
ssiuser@vagrant:~/Desktop/ssi_labs/lab_exam$ sudo fail2ban-client set vsftpd unbanip 192.168.66.6
192.168.66.6
ssiuser@vagrant:~/Desktop/ssi_labs/lab_exam$ sudo fail2ban-client status vsftpd
Status for the jail: vsftpd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     10
|  `- File list:        /var/log/vsftpd.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
   `- Banned IP list:
```

Ejercicio 2.

```
ssiuser@vagrant:~/Desktop/ssi_labs/lab_exam$ crunch 10 10 -t test%%%... -o dict.txt
çCrunch will now generate the following amount of data: 11000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1000

crunch: 100% completed generating output
ssiuser@vagrant:~/Desktop/ssi_labs/lab_exam$ cp /etc/passwd passwd
ssiuser@vagrant:~/Desktop/ssi_labs/lab_exam$ cp /etc/shadow shadow
cp: cannot open '/etc/shadow' for reading: Permission denied
ssiuser@vagrant:~/Desktop/ssi_labs/lab_exam$ sudo cp /etc/shadow shadow
ssiuser@vagrant:~/Desktop/ssi_labs/lab_exam$ unshadow passwd shadow > johnFile.txt
fopen: shadow: Permission denied
ssiuser@vagrant:~/Desktop/ssi_labs/lab_exam$ sudo unshadow passwd shadow > johnFile.txt
ssiuser@vagrant:~/Desktop/ssi_labs/lab_exam$ john johnFile.txt --wordlist=dict.txt
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
test123...       (user3)
test121...       (user1)
test122...       (user2)
3g 0:00:00:06 100% 0.4405g/s 146.8p/s 525.1c/s 525.1C/s test960.....test999...
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Ejercicio 3.

Primero se debe importar la clave privada del usuario 3, ya que, al ser el receptor del mensaje, el usuario 1 (emisor) ha cifrado dicho mensaje con nuestra clave pública, por lo que, el descifrado debe ser con la clave privada, por lo que, se importa con *gpg –import private_key_user3.asc*.

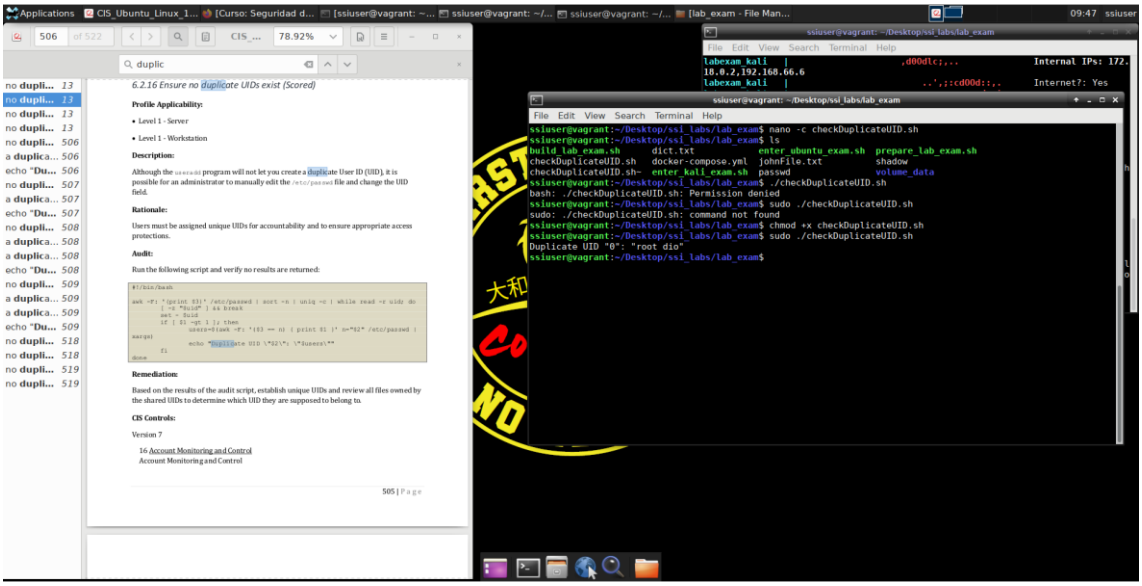
Se podría hacer directamente el descifrado, no obstante, es recomendable comprobar que la clave se ha importado correctamente con *gpg –list-secret-keys*. Una vez hecho esto, se descifra el mensaje con el comando *gpg –o decypheredMessage.txt –d mensaje_de_1_a_3.txt.asc*, y automáticamente se podrá leer el contenido del mensaje previamente cifrado.

Esta explicación puede verse en la siguiente captura:

```
ssiuser@vagrant:~/tmp$ gpg --import
mensaje_de_1_a_3.txt.asc  private_key_user3.asc     public_key_user3.asc
private_key_user1.asc     public_key_user1.asc
ssiuser@vagrant:~/tmp$ gpg --import private_key_user3.asc
gpg: /home/ssiuser/.gnupg/trustdb.gpg: trustdb created
gpg: key 3291AB667484E9C2: public key "Usuario3 <user3@uniovi.es>" imported
gpg: key 3291AB667484E9C2: secret key imported
gpg: Total number processed: 1
gpg:               imported: 1
gpg:       secret keys read: 1
gpg:   secret keys imported: 1
ssiuser@vagrant:~/tmp$ gpg --list-secret-keys
/home/ssiuser/.gnupg/pubring.kbx
--------------------------------
sec   rsa3072 2023-05-23 [SC] [expires: 2025-05-22]
      04B673A95862A4A7F46FE9C93291AB667484E9C2
uid           [ unknown] Usuario3 <user3@uniovi.es>
ssb   rsa3072 2023-05-23 [E] [expires: 2025-05-22]

ssiuser@vagrant:~/tmp$ gpg -o decypheredMessage.txt -d mensaje_de_1_a_3.txt.asc
gpg: encrypted with 3072-bit RSA key, ID E97E4BB1DA86E1B5, created 2023-05-23
      "Usuario3 <user3@uniovi.es>"
ssiuser@vagrant:~/tmp$ ls
decypheredMessage.txt     private_key_user1.asc  public_key_user1.asc
mensaje_de_1_a_3.txt.asc  private_key_user3.asc  public_key_user3.asc
ssiuser@vagrant:~/tmp$ cat decypheredMessage.txt
Este examen !! Lo vamos a aprobar!!

ssiuser@vagrant:~/tmp$
```

Ejercicio 4.

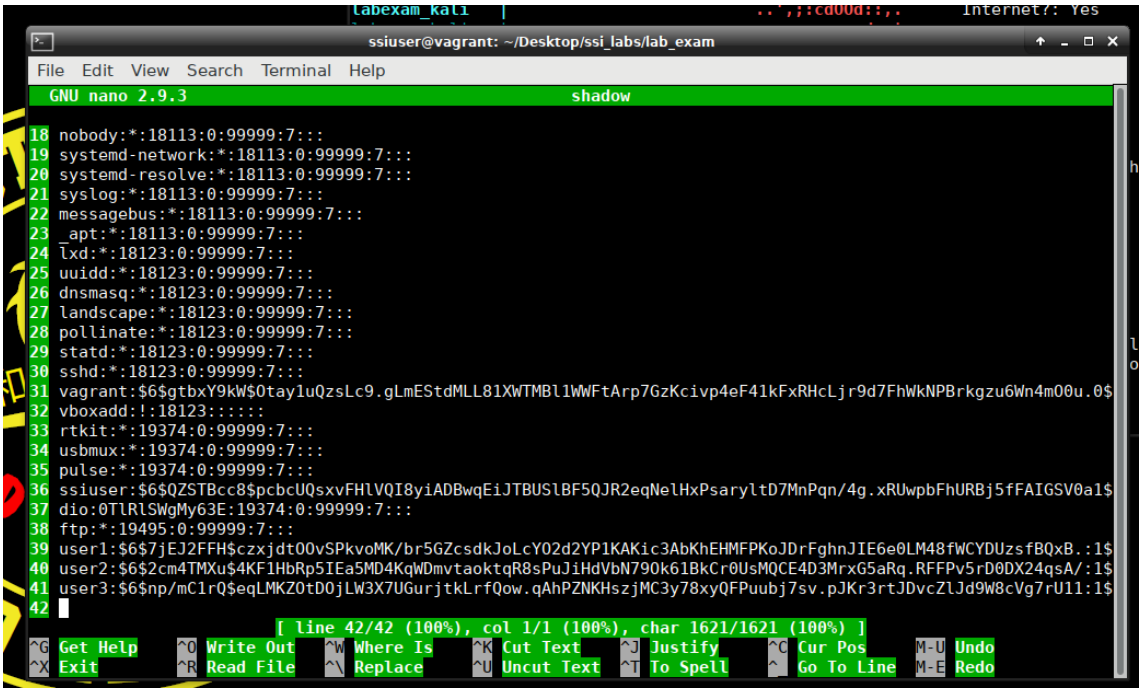
a. Se ha seguido el control *6.2.16 Ensure no duplicate UIDs exist (Scored)* en el CIS, y el resultado de ejecutar el script ha sido:

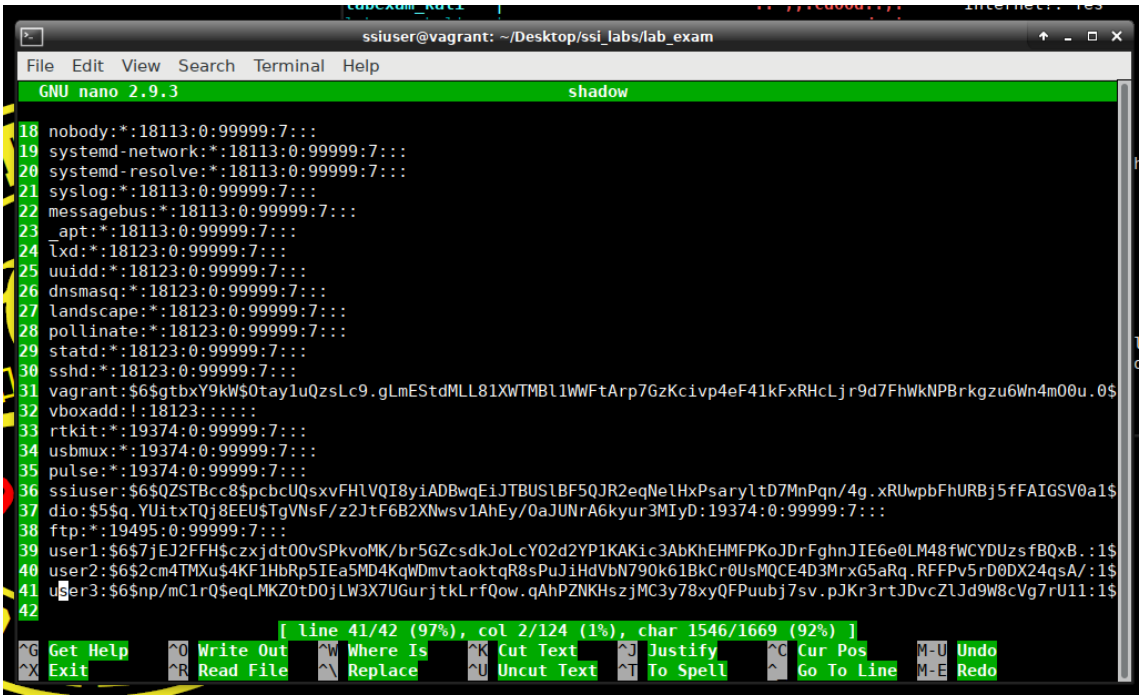


b. Para ello, primero generamos la contraseña con la encriptación correcta, es decir, sha256, utilizamos el comando mkpasswd –m sha-256 aversiapruebo.

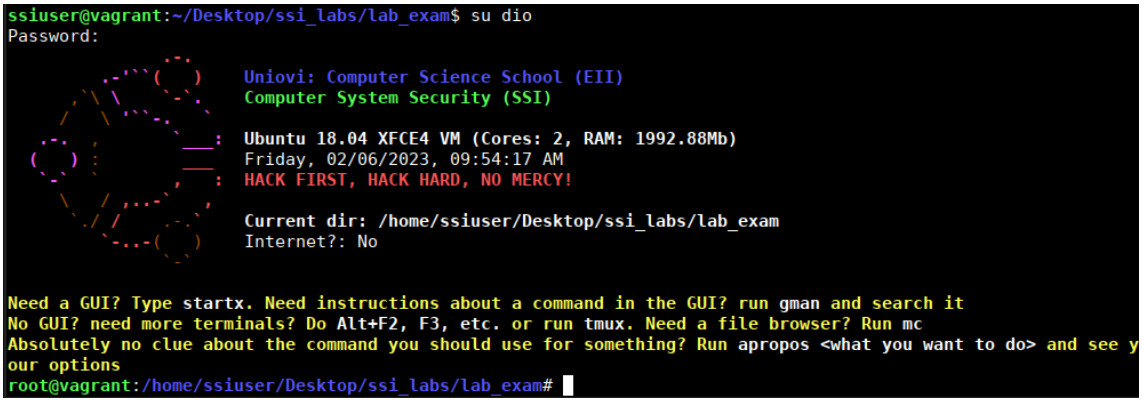
```
ssiuser@vagrant:~/Desktop/ssi_labs/lab_exam$ mkpasswd -m sha-256 aversiapruebo
$5$q.YUitxTQj8EEU$TgVNsF/z2JtF6B2XNwsv1AhEy/OaJUNrA6kyur3MIyD
```

Se edita el fichero shadow con la nueva contraseña.

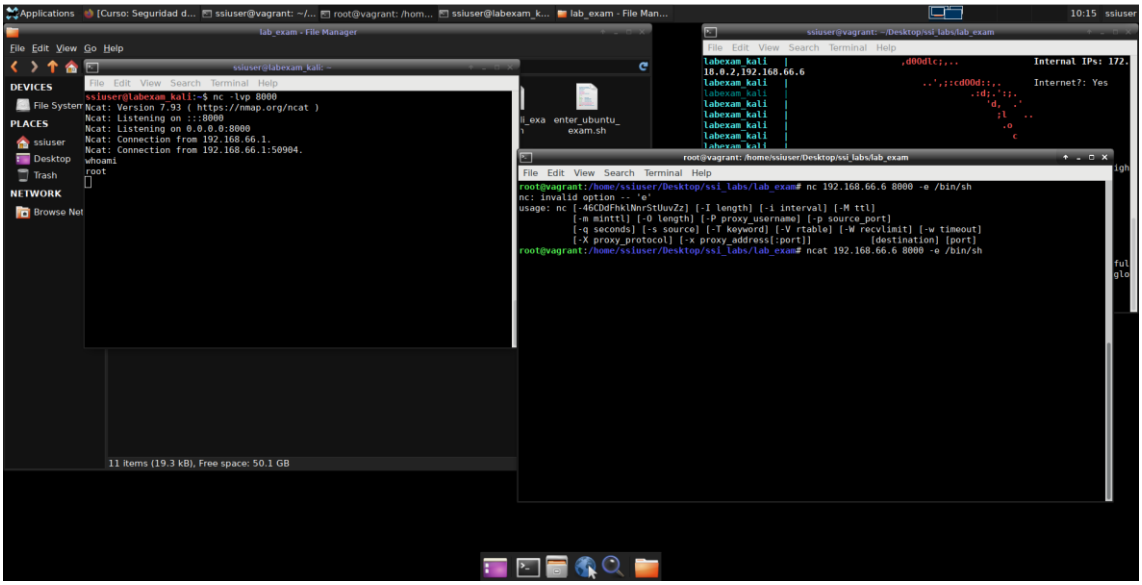




c. Entramos en sesión como el usuario dio, con la contraseña definida anteriormente



Posteriormente, se hace un reverse shell, escuchando en la máquina atacante, y se ve que, al ejecutar whoami, somos el usuario al que hemos accedido antes.



Ejercicio 5.

```
root@vagrant:/home/ssiuser/Desktop/ssi_labs/lab_exam# nmap -sV 192.168.66.3

Starting Nmap 7.60 ( https://nmap.org ) at 2023-06-02 10:18 CEST
Nmap scan report for 192.168.66.3
Host is up (0.000015s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
23/tcp open  telnet  Linux telnetd
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 02:42:C0:A8:42:03 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.54 seconds
```

- A la lista de vulnerabilidades en el CVE.
- Utilizar una base de datos de exploits en la que buscar dichos servicios y versiones.
- Metasploit.

```
msssiuser@labexam_kali:~$ msfconsole -q
msf6 > search apache

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

   #    Name                                                      Disclosure Date  Rank       Check  Description
   -    ----                                                      ---------------  ----       -----  -----------
   0    exploit/multi/http/apache_apisix_api_default_token_rce    2020-12-07       excellent  Yes    APISIX Admin API default access t
oken RCE
   1    exploit/linux/http/atutor_filemanager_traversal           2016-03-01       excellent  Yes    ATutor 2.2.1 Directory Traversal
/ Remote Code Execution
   2    exploit/multi/http/apache_activemq_upload_jsp             2016-06-01       excellent  No     ActiveMQ web shell upload
   3    auxiliary/scanner/http/apache_userdir_enum                                  normal     No     Apache "mod_userdir" User Enumera
tion
   4    exploit/multi/http/apache_normalize_path_rce              2021-05-10       excellent  Yes    Apache 2.4.49/2.4.50 Traversal RC
E
   5    auxiliary/scanner/http/apache_normalize_path              2021-05-10       normal     No     Apache 2.4.49/2.4.50 Traversal RC
E scanner
   6    exploit/windows/http/apache_activemq_traversal_upload     2015-08-19       excellent  Yes    Apache ActiveMQ 5.x-5.11.1 Direct
ory Traversal Shell Upload
   7    auxiliary/scanner/http/apache_activemq_traversal                            normal     No     Apache ActiveMQ Directory Travers
al
   8    auxiliary/scanner/http/apache_activemq_source_disclosure                    normal     No     Apache ActiveMQ JSP Files Source
Disclosure
   9    auxiliary/scanner/http/axis_login                                           normal     No     Apache Axis2 Brute Force Utility
   10   auxiliary/scanner/http/axis_local_file_include                              normal     No     Apache Axis2 v1.4.1 Local File In
clusion
   11   auxiliary/dos/http/apache_commons_fileupload_dos          2014-02-06       normal     No     Apache Commons FileUpload and Apa
che Tomcat DoS
   12   exploit/linux/http/apache_continuum_cmd_exec              2016-04-06       excellent  Yes    Apache Continuum Arbitrary Comman
d Execution
   13   exploit/linux/http/apache_couchdb_cmd_exec                2016-04-06       excellent  Yes    Apache CouchDB Arbitrary Command
Execution
   14   exploit/multi/http/apache_couchdb_erlang_rce              2022-01-21       excellent  Yes    Apache Couchdb Erlang RCE
   15   exploit/linux/http/apache_druid_js_rce                    2021-01-21       excellent  Yes    Apache Druid 0.20.0 Remote Comman
d Execution
   16   exploit/multi/http/apache_flink_jar_upload_exec           2019-11-13       excellent  Yes    Apache Flink JAR Upload Java Code
```

```
d Vulnerability
   103  exploit/linux/http/rconfig_ajaxarchivefiles_rce          2020-03-11       good       Yes    Rconfig 3.x Chained Remote Code E
xecution
   104  exploit/linux/http/piranha_passwd_exec                   2000-04-04       excellent  No     RedHat Piranha Virtual Server Pac
kage passwd.php3 Arbitrary Command Execution
   105  exploit/unix/webapp/spip_connect_exec                    2012-07-04       excellent  Yes    SPIP connect Parameter PHP Inject
ion
   106  exploit/unix/misc/spamassassin_exec                      2006-06-06       excellent  No     SpamAssassin spamd Remote Command
 Execution
   107  exploit/multi/http/spring_framework_rce_spring4shell     2022-03-31       manual     Yes    Spring Framework Class property R
CE (Spring4Shell)
   108  exploit/linux/http/symantec_web_gateway_lfi              2012-05-17       excellent  Yes    Symantec Web Gateway 5.0.2.8 relf
ile File Inclusion Vulnerability
   109  auxiliary/admin/http/tomcat_administration                                  normal     No     Tomcat Administration Tool Defaul
t Access
   110  auxiliary/scanner/http/tomcat_mgr_login                                     normal     No     Tomcat Application Manager Login
Utility
   111  exploit/multi/http/tomcat_jsp_upload_bypass               2017-10-03       excellent  Yes    Tomcat RCE via JSP Upload Bypass
   112  auxiliary/admin/http/tomcat_utf8_traversal                2009-01-09       normal     No     Tomcat UTF-8 Directory Traversal
Vulnerability
   113  exploit/linux/http/trendmicro_websecurity_exec            2020-06-10       excellent  Yes    Trend Micro Web Security (Virtual
 Appliance) Remote Code Execution
   114  auxiliary/admin/http/trendmicro_dlp_traversal             2009-01-09       normal     No     TrendMicro Data Loss Prevention 5
.5 Directory Traversal
   115  exploit/linux/http/vmware_view_planner_4_6_uploadlog_rce  2021-03-02       excellent  Yes    VMware View Planner Unauthenticat
ed Log File Upload RCE
   116  auxiliary/scanner/http/wangkongbao_traversal                                normal     No     WANGKONGBAO CNS-1000 and 1100 UTM
 Directory Traversal
   117  post/windows/gather/enum_tomcat                                             normal     No     Windows Gather Apache Tomcat Enum
eration
   118  exploit/unix/webapp/wp_phpmailer_host_header              2017-05-03       average    Yes    WordPress PHPMailer Host Header C
ommand Injection
   119  exploit/unix/webapp/jquery_file_upload                    2018-10-09       excellent  Yes    blueimp's jQuery (Arbitrary) File
 Upload


Interact with a module by name or index. For example info 119, use 119 or use exploit/unix/webapp/jquery_file_upload

msf6 >
```

Ejercicio 6.