

Proyecto Módulo 2

Cabrera Balderas Carlos Eduardo
Gonzalez Vargas Andrea Itzel

23/03/2018


Índice

1. Manual de usuario	2	1.7. Sección de monitoreo de almace-	
1.1. Login	2	namiento	5
1.2. Dashboard	2	1.8. Sección de monitoreo de archivos	
1.3. Sección de monitoreo de usuarios	3	y sockets	5
1.4. Sección de monitoreo de procesos	3	1.9. Sección de monitoreo de servidor	
1.5. Sección de monitoreo de red . . .	4	web	6
1.6. Sección de monitoreo de autenti-		1.10. Secciones personalizadas	8
cación	4	1.11. Archivo de configuración	8
		1.12. Administrar cuentas de usuario .	9

1. Manual de usuario

1.1. Login

Para iniciar sesión se tiene que contar con credenciales válidas, se ingresan y le da en *Iniciar Sesión* para iniciar sesión con su usuario.



The logo for UNAM CERT is centered at the top. It features a blue shield with a white keyhole in the center, containing a red dot. Above the shield are two blue horse heads facing each other. Below the shield, the text 'UNAM' is written in a large, blue, serif font, and 'CERT' is written below it in a smaller, blue, serif font.

1.2. Dashboard

Es la ventana principal, por lo tanto, es lo que primero verá el usuario al acceder a su cuenta, contando con características como la distribución, arquitectura y nombre del equipo, dominio y las tareas de cron que existen en el sistema.

Podemos acceder a las demás secciones dando click en la parte superior izquierda en el menú y eligiendo la sección deseada.

Dashboard

Distribución: Ubuntu 16.04.3 LTS
Arquitectura: x86_64
Nombre de equipo: chepe
Nombre de dominio: (none)

Tareas de cron:

Sistema:

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
17 * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.daily)
47 6 * * 7 root test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.weekly)
52 6 1 * * root test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.monthly)

Usuario chepe:

0 5 * * 1 ls

1.3. Sección de monitoreo de usuarios

Es la primera sección y, en esta, se muestran todos los usuarios del sistema con sus respectivos grupos, así como los usuarios activos y bloqueados.

Monitoreo de usuarios

USUARIOS Y GRUPOS

USUARIOS ACTIVOS

Usuario: Grupos

root: root

daemon: daemon

bin: bin

sys: sys

sync: nogroup

games: games

man: man

lp: lp

mail: mail

news: news

uucp: uucp

proxy: proxy

www-data: www-data

backup: backup

list: list

irc: irc

gnats: gnats

nobody: nogroup

systemd-timesync: systemd-timesync

systemd-network: systemd-network

systemd-resolve: systemd-resolve

systemd-bus-proxy: systemd-bus-proxy

syslog: syslog adm

_apt: nogroup

messagebus: messagebus

uidd: uidd

lightdm: lightdm

whoopsie: whoopsie

avahi-autoipd: avahi-autoipd

avahi: avahi

dnsmasq: dnsmasq

dnsmasq: nogroup

Usuarios bloqueados

daemon

bin

sys

sync

games

man

lp

mail

news

uucp

proxy

www-data

backup

list

irc

gnats

nobody

systemd-timesync

systemd-network

systemd-resolve

systemd-bus-proxy

syslog

_apt

messagebus

uidd

lightdm

whoopsie

avahi-autoipd

avahi

dnsmasq

colord

speech-dispatcher

1.4. Sección de monitoreo de procesos

En dicha sección se podrán visualizar los procesos actuales del sistema con características como el PID, usuario, CPU, uso de memoria por proceso y el nombre del proceso.

Se puede hacer búsqueda textual o por expresión regular para filtrar la información y tener algo más específico a lo que se requiere.

3

EDITAR DATOS

ADMINISTRAR USUARIOS

ADMINISTRAR SECCIONES

UNAM CERT

Monitoreo de procesos

FILTRAR

Búsqueda textual

Búsqueda por expresión regular

ACEPTAR

PID	UID	USER	%CPU	%MEM	CMD
1	0	root	0.1	0.0	/sbin/init splash
2	0	root	0.0	0.0	[kthreadd]
3	0	root	0.0	0.0	[ksoftirqd/0]
5	0	root	0.0	0.0	[kworker/0:0H]
7	0	root	0.1	0.0	[rcu_sched]
8	0	root	0.0	0.0	[rcu_bh]
9	0	root	0.0	0.0	[migration/0]
10	0	root	0.0	0.0	[watchdog/0]
11	0	root	0.0	0.0	[watchdog/1]
12	0	root	0.0	0.0	[migration/1]
13	0	root	0.0	0.0	[ksoftirqd/1]
15	0	root	0.0	0.0	[kworker/1:0H]
16	0	root	0.0	0.0	[watchdog/2]
17	0	root	0.0	0.0	[migration/2]
18	0	root	0.0	0.0	[ksoftirqd/2]
20	0	root	0.0	0.0	[kworker/2:0H]
21	0	root	0.0	0.0	[watchdog/3]
22	0	root	0.0	0.0	[migration/3]
23	0	root	0.0	0.0	[ksoftirqd/3]
25	0	root	0.0	0.0	[kworker/3:0H]
26	0	root	0.0	0.0	[watchdog/4]
27	0	root	0.0	0.0	[migration/4]

1.5. Sección de monitoreo de red

Aquí se puede encontrar información de la red como la ip, el gateway, los puertos escucha en TCP/UDP, las conexiones, estadísticas y las reglas de iptables entre otros.

EDITAR DATOS

ADMINISTRAR USUARIOS

ADMINISTRAR SECCIONES

UNAM CERT

Monitoreo de red

INTERFACES Y PUERTOS

CONEXIONES

IPTABLES

ESTADÍSTICAS

Interfaz IP/Máscara Gateway

```
wlp3s0 192.168.100.23/24 192.168.100.1
wlp3s0 192.168.100.23/24 0.0.0.0
wlp3s0 192.168.100.23/24 0.0.0.0
vmnet1 172.16.163.1/24 0.0.0.0
vmnet2 192.168.1.1/24 0.0.0.0
vmnet8 192.168.42.1/24 0.0.0.0
virbr0 192.168.122.1/24 0.0.0.0
```

Puertos en escucha

tcp	0	0	127.0.0.1:631	0.0.0.0:*	LISTEN	5083/cupsd
tcp	0	0	0.0.0.0:25	0.0.0.0:*	LISTEN	2529/master
tcp	0	0	127.0.0.1:9050	0.0.0.0:*	LISTEN	1197/tor
tcp	0	0	0.0.0.0:443	0.0.0.0:*	LISTEN	2093/vmware-hostd
tcp	0	0	0.0.0.0:17500	0.0.0.0:*	LISTEN	3394/dropbox
tcp	0	0	127.0.0.1:8000	0.0.0.0:*	LISTEN	8033/python3
tcp	0	0	127.0.0.1:17600	0.0.0.0:*	LISTEN	3394/dropbox
tcp	0	0	127.0.0.1:17603	0.0.0.0:*	LISTEN	3394/dropbox
tcp	0	0	0.0.0.0:389	0.0.0.0:*	LISTEN	1399/slappd
tcp	0	0	0.0.0.0:902	0.0.0.0:*	LISTEN	1696/vmware-authdla
tcp	0	0	127.0.0.1:11211	0.0.0.0:*	LISTEN	1140/memcached
tcp	0	0	0.0.0.0:2222	0.0.0.0:*	LISTEN	1142/ssh
tcp	0	0	0.0.0.0:7890	0.0.0.0:*	LISTEN	3053/goaccess
tcp	0	0	127.0.0.1:8307	0.0.0.0:*	LISTEN	2093/vmware-hostd
tcp	0	0	127.0.0.1:53	0.0.0.0:*	LISTEN	2757/dnsmasq
tcp	0	0	192.168.122.1:53	0.0.0.0:*	LISTEN	2292/dnsmasq
tcp6	0	0	:::1:631	:::*	LISTEN	5083/cupsd
tcp6	0	0	:::25	:::*	LISTEN	2529/master
tcp6	0	0	:::443	:::*	LISTEN	2093/vmware-hostd
tcp6	0	0	:::17500	:::*	LISTEN	3394/dropbox
tcp6	0	0	:::389	:::*	LISTEN	1399/slappd

1.6. Sección de monitoreo de autenticación

En esta sección se podrá ver la bitácora de auth.log de manera *cruda* pero permitiendo búsquedas específicas para depurar la información que queremos obtener del archivo.

4

EDITAR DATOS

ADMINISTRAR USUARIOS

ADMINISTRAR SECCIONES

UNAM CERT

Bitácora auth.log

Ubicación: /var/log/auth.log

FILTRAR

Número máximo de líneas

Búsqueda textual

Búsqueda por expresión regular

ACEPTAR

```

Mar 23 10:09:02 chepe sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 23 10:09:02 chepe sudo: pam_unix(sudo:session): session closed for user root
Mar 23 10:09:02 chepe sudo: root : TTY=pts/2 ; PWD=/home/chepe/Documents/fac/cert/2Prog0rSeg/proy/proyecto ; USER=root ; COMMAND=/usr/bin/passwd -S kernoops
Mar 23 10:09:02 chepe sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 23 10:09:02 chepe sudo: pam_unix(sudo:session): session closed for user root
Mar 23 10:09:02 chepe sudo: root : TTY=pts/2 ; PWD=/home/chepe/Documents/fac/cert/2Prog0rSeg/proy/proyecto ; USER=root ; COMMAND=/usr/bin/passwd -S pulse
Mar 23 10:09:02 chepe sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 23 10:09:02 chepe sudo: pam_unix(sudo:session): session closed for user root
Mar 23 10:09:02 chepe sudo: root : TTY=pts/2 ; PWD=/home/chepe/Documents/fac/cert/2Prog0rSeg/proy/proyecto ; USER=root ; COMMAND=/usr/bin/passwd -S rtkit
Mar 23 10:09:02 chepe sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 23 10:09:02 chepe sudo: pam_unix(sudo:session): session closed for user root
Mar 23 10:09:02 chepe sudo: root : TTY=pts/2 ; PWD=/home/chepe/Documents/fac/cert/2Prog0rSeg/proy/proyecto ; USER=root ; COMMAND=/usr/bin/passwd -S saned
Mar 23 10:09:02 chepe sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 23 10:09:02 chepe sudo: pam_unix(sudo:session): session closed for user root
Mar 23 10:09:02 chepe sudo: root : TTY=pts/2 ; PWD=/home/chepe/Documents/fac/cert/2Prog0rSeg/proy/proyecto ; USER=root ; COMMAND=/usr/bin/passwd -S usbmux
Mar 23 10:09:02 chepe sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 23 10:09:02 chepe sudo: pam_unix(sudo:session): session closed for user root
Mar 23 10:09:02 chepe sudo: root : TTY=pts/2 ; PWD=/home/chepe/Documents/fac/cert/2Prog0rSeg/proy/proyecto ; USER=root ; COMMAND=/usr/bin/passwd -S chepe
Mar 23 10:09:02 chepe sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 23 10:09:02 chepe sudo: pam_unix(sudo:session): session closed for user root

```

1.7. Sección de monitoreo de almacenamiento

Sección que nos da una vista de las particiones actuales del disco, su capacidad usado y libre, así como la visualización de la memoria RAM y del CPU con los mismos fines.

EDITAR DATOS

ADMINISTRAR USUARIOS

ADMINISTRAR SECCIONES

UNAM CERT

Monitoreo de almacenamiento

Particiones

Filesystem	Size	Used	Avail	Use%	Mounted on
udev	3.9G	0	3.9G	0%	/dev
tmpfs	787M	18M	770M	3%	/run
/dev/sda5	904G	182G	677G	22%	/
tmpfs	3.9G	65M	3.8G	2%	/dev/shm
tmpfs	5.0M	4.0K	5.0M	1%	/run/lock
tmpfs	3.9G	0	3.9G	0%	/sys/fs/cgroup
/dev/sda1	1.2G	4.5M	1.2G	1%	/boot/efi
cgmfs	100K	0	100K	0%	/run/cgmanager/fs
tmpfs	787M	64K	787M	1%	/run/user/1000

Memoria RAM

	total	used	free	shared	buff/cache	available
Mem:	7.7G	2.7G	2.1G	561M	2.9G	4.1G
Swap:	11G	0B	11G			

CPU

Linux 4.4.0-116-generic (chepe) 23/03/18 _x86_64_ (8 CPU)

	CPU	%usr	%nice	%sys	%iowait	%irq	%soft	%steal	%guest	%gnice	%idle
10:10:14	all	1.86	0.03	0.70	0.00	0.00	0.00	0.00	0.00	0.00	96.61

Total usado: 3.39%

Total libre: 96.61%

1.8. Sección de monitoreo de archivos y sockets

La sección nos mostrará los archivos abiertos, con todos sus campos de información como su proceso asociado y el usuario que los está ejecutando.

A la vez, nos da una manera de filtrar esta información para la comodidad del usuario.

5

EDITAR DATOS

ADMINISTRAR USUARIOS

ADMINISTRAR SECCIONES

UNAM CERT

Monitoreo de archivos y sockets

FILTRAR

Número máximo de líneas

Búsqueda textual

Búsqueda por expresión regular

ACEPTAR

COMMAND	PID	TID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE NAME
systemd	1		root	cwd	DIR	8,5	4096	2 /
systemd	1		root	rtd	DIR	8,5	4096	2 /
systemd	1		root	txt	REG	8,5	1577232	4719006 /lib/systemd/systemd
systemd	1		root	mem	REG	8,5	18976	4718872 /lib/x86_64-linux-gnu/libuuid.so.1.3.0
systemd	1		root	mem	REG	8,5	262408	4723515 /lib/x86_64-linux-gnu/libblkid.so.1.1.0
systemd	1		root	mem	REG	8,5	14608	4728155 /lib/x86_64-linux-gnu/libl-2.23.so
systemd	1		root	mem	REG	8,5	456632	4723461 /lib/x86_64-linux-gnu/libpcre.so.3.13.2
systemd	1		root	mem	REG	8,5	1868984	4728153 /lib/x86_64-linux-gnu/libc-2.23.so
systemd	1		root	mem	REG	8,5	138696	4728152 /lib/x86_64-linux-gnu/libpthread-2.23.so
systemd	1		root	mem	REG	8,5	286824	4718619 /lib/x86_64-linux-gnu/libmount.so.1.1.0
systemd	1		root	mem	REG	8,5	64144	4718812 /lib/x86_64-linux-gnu/libapparmor.so.1.4.0
systemd	1		root	mem	REG	8,5	92864	4719904 /lib/x86_64-linux-gnu/libkmod.so.2.3.0
systemd	1		root	mem	REG	8,5	117288	4723322 /lib/x86_64-linux-gnu/libaudit.so.1.0.0
systemd	1		root	mem	REG	8,5	55904	4723448 /lib/x86_64-linux-gnu/libpam.so.0.83.1
systemd	1		root	mem	REG	8,5	288848	4718638 /lib/x86_64-linux-gnu/libseccomp.so.2.3.1
systemd	1		root	mem	REG	8,5	31712	4728171 /lib/x86_64-linux-gnu/librt-2.23.so
systemd	1		root	mem	REG	8,5	23128	4723335 /lib/x86_64-linux-gnu/libcap.so.2.24
systemd	1		root	mem	REG	8,5	130224	4723490 /lib/x86_64-linux-gnu/libeLinux.so.1
systemd	1		root	mem	REG	8,5	162632	4728151 /lib/x86_64-linux-gnu/ld-2.23.so

1.9. Sección de monitoreo de servidor web

Finalmente, en esta sección podemos obtener los módulos y VirtualHost de Apache habilitados.

EDITAR DATOS

ADMINISTRAR USUARIOS

ADMINISTRAR SECCIONES

UNAM CERT

Monitoreo del servidor web

GRÁFICAS Y ESTADÍSTICAS

MÓDULOS Y VIRTUALHOSTS

BITÁCORAS

Loaded Modules:
core_module (static)
so_module (static)
watchdog_module (static)
http_module (static)
log_config_module (static)
logio_module (static)
version_module (static)
unixd_module (static)
access_compat_module (shared)
actions_module (shared)
alias_module (shared)
auth_basic_module (shared)
auth_digest_module (shared)
authn_core_module (shared)
authn_file_module (shared)
authnz_ldap_module (shared)
authz_core_module (shared)
authz_host_module (shared)
authz_user_module (shared)
autoindex_module (shared)
cgi_module (shared)
cgid_module (shared)
deflate_module (shared)
dir_module (shared)
env_module (shared)
filter_module (shared)
headers_module (shared)
info_module (shared)
ldap_module (shared)
mime_module (shared)
mpm_prefork_module (shared)

VirtualHost configuration:
*:6888 127.0.1.1 (/etc/apache2/sites-enabled/web-ip.conf:1)
*:80 becarios.cert.unam.mx (/etc/apache2/sites-enabled/wordpress.conf:1)
*:443 becarios.cert.unam.mx (/etc/apache2/sites-enabled/wordpress.conf:21)

Además, de que contará con una pestaña llamada *Bitácoras* donde podremos elegir entre las bitácoras de Apache y otras, desplegando así una lista de los logs que se pueden mostrar, tales como: Messages, Syslog, PostgreSQL, MySQL, y ModSecurity.

6

Monitoreo del servidor web

GRÁFICAS Y ESTADÍSTICAS

MÓDULOS Y VIRTUALHOSTS

BITÁCORAS

ACCESO DE APACHE

/var/log/apache2/access.log

ERROR DE APACHE

/var/log/apache2/error.log

APACHE MOD SECURITY

Mod Security

OTRAS

Syslog

Messages

PostgreSQL

MySQL

En las bitácoras de acceso de Apache se tiene la opción de mostrar con un formato definido la salida presentada, lo cual se hace por medio de una entrada en el campo **Formato** que debe tener la forma [hlutrsbRU]+.

Bitácora de acceso de Apache

Ubicación: /var/log/apache2/access.log

FILTRAR

Número máximo de líneas

Búsqueda textual

Búsqueda por expresión regular

Formato

?

ACEPTAR

127.0.0.1 - - [15/Mar/2018:08:14:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"

127.0.0.1 - - [15/Mar/2018:08:19:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"

127.0.0.1 - - [15/Mar/2018:08:24:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"

127.0.0.1 - - [15/Mar/2018:08:29:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"

127.0.0.1 - - [15/Mar/2018:08:34:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"

127.0.0.1 - - [15/Mar/2018:08:39:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"

127.0.0.1 - - [15/Mar/2018:08:44:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"

127.0.0.1 - - [15/Mar/2018:08:49:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"

127.0.0.1 - - [15/Mar/2018:08:54:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"

127.0.0.1 - - [15/Mar/2018:08:59:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"

127.0.0.1 - - [15/Mar/2018:09:04:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"

127.0.0.1 - - [15/Mar/2018:09:09:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"

127.0.0.1 - - [15/Mar/2018:09:14:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"

127.0.0.1 - - [15/Mar/2018:09:19:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"

127.0.0.1 - - [15/Mar/2018:09:24:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"

127.0.0.1 - - [15/Mar/2018:09:29:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"

127.0.0.1 - - [15/Mar/2018:09:34:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"

127.0.0.1 - - [15/Mar/2018:09:39:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"

Cada letra del formato representa un campo de la bitácora de acceso, de manera que se muestran estos en el orden indicado.

Formato

?

Formato aceptado
h - host
l - identd
u - userid
t - fecha
r - petición
s - código de respuesta
b - tamaño
R - referer
U - agente de usuario

Ejemplo:
r t s U h

ACEPTAR

1.10. Secciones personalizadas

EDITAR DATOS
ADMINISTRAR USUARIOS
ADMINISTRAR SECCIONES
UNAM CERT

Sección 1

BITÁCORAS
/var/log/auth.log
/var/log/bootstrap.log
/home/chepe/cert2/proy/proyecto/conf/hola
/home/chepe/cert2/proy/proyecto/conf/hola' && ls && echo `

En esta sección se muestran las bitácoras que se especificaron en el archivo de configuración para alguna sección personalizada.

1.11. Archivo de configuración

En el archivo de configuración se debe especificar las rutas de las bitácoras para las secciones que lo requieran. El formato del archivo es el siguiente:

```
[seccion]
```

```
archivo = /ruta/del/archivo
```

```
[seccion_2]
```

```
archivo_2 = /otra/ruta
```

Las secciones que requieren rutas para sus bitácoras son **web**, **autenticacion** y las secciones personalizadas, de manera que para estas últimas, el nombre de la sección que será especificada en el archivo de configuración será el **Nombre de configuración** que tenga asociado cada una, es decir, si se creó la sección que tiene por título “Sección de prueba 1”, con **Nombre de configuración** **seccion_1**, entonces en el archivo de configuración se debe de especificar como:


```
[seccion_1]
```

```
archivo1=/ruta/del/archivo
```

```
...
```

La sección de monitoreo de autenticación debe de especificar la ruta de su bitácora de la siguiente manera:

```
[autenticacion]
```

```
auth = /var/log/auth.log
```

Y las bitácoras de la sección de monitoreo web deben de ser especificadas como se indica:

```
[web]
```

```
mod_sec = /var/log/apache2/modsec_audit.log
```

```
syslog = /var/log/syslog
```

```
messages = /var/log/messages
```

```
postgres = /var/log/postgresql/postgresql-9.6-main.log
```

```
mysql = /var/log/mysql/error.log
```

Sólo en el caso de las secciones personalizadas es irrelevante el nombre de las variables de cada archivo, sin embargo, en las otras secciones (**web** y **autenticacion**), es importante que se utilicen los nombres definidos.

Un ejemplo completo de un archivo de configuración es el siguiente:

```
[autenticacion]
```

```
auth = /var/log/auth.log
```

```
[web]
```

```
mod_sec = /var/log/apache2/modsec_audit.log
```

```
syslog = /var/log/syslog
```

```
messages = /var/log/messages
```

```
postgres = /var/log/postgresql/postgresql-9.6-main.log
```

```
mysql = /var/log/mysql/error.log
```

```
[seccion_1]
```

```
archivo1 = /var/log/auth.log
```

```
archivo2 = /var/log/bootstrap.log
```

```
archivo3 = /home/chepe/cert2/proy/proyecto/conf/hola
```

```
archivo4 = /home/chepe/cert2/proy/proyecto/conf/hola' && ls && echo 'j
```

1.12. Administrar cuentas de usuario

En la barra superior en la parte derecha tendremos la opción de administrar las cuentas a manera de poder crear o eliminar a nuestro gusto.

[EDITAR DATOS](#) [ADMINISTRAR USUARIOS](#) [ADMINISTRAR SECCIONES](#)

Editar datos

Nombre de usuario

admin

Nombre

Admin

Apellido

Dirección de correo electrónico

admin@localhost

[Cambiar contraseña](#)

ACEPTAR

En esta sección podemos obtener los módulos y VirtualHost de Apache habilitados. Además, de que contiene la pestaña llamada bitácoras donde podremos elegir entre las bitácoras de Apache y otras, desplegando así una lista de los logs que se pueden mostrar, tales como: Messages, Syslog, POstgreSQL, MySQL y ModSecurity.

≡

[EDITAR DATOS](#) [ADMINISTRAR USUARIOS](#) [ADMINISTRAR SECCIONES](#)

Usuarios

+

ADMIN

Nombre: Admin


Correo: admin@localhost


Fecha de registro: 16 de Marzo de 2018 a las 19:11

Último inicio de sesión: 23 de Marzo de 2018 a las 10:08


En la barra superior derecha tenemos también la opción de administrar las cuentas de los usuarios, se listarán con la opción de administrar las cuentas de los usuarios, se listarán con la opción de eliminar la cuenta justo debajo de cada una.

Hasta arriba de las cuentas se podrán agregar más dando click en el +, donde tenemos que llenar el nombre de usuario, el nombre y apellido, correo, contraseña y una confirmación de la misma.



EDITAR DATOSADMINISTRAR USUARIOSADMINISTRAR SECCIONES


Secciones personalizadas




SECCIÓN 1



Nombre de configuración: seccion_1

Fecha de creación: 17 de Marzo de 2018 a las 19:01



En esta opción podemos ver la secciones que hemos creado con su respectivo nombre, nombre de configuración y fecha de creación, teniendo las mismas opciones de agregar, eliminar y editar a cada una de ellas.



EDITAR DATOSADMINISTRAR USUARIOSADMINISTRAR SECCIONES

Nueva sección

Título

Nombre de configuración

CREAR SECCIÓN

En caso de querer agregar una nueva sección se deberá especificar el título, nombre de configuración y dar click en el botón de crear sección.