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	web	6
	1.5. Sección de monitoreo de red	4	1.10. Secciones personalizadas	
	1.6. Sección de monitoreo de autenti-		1.11. Archivo de configuración	8
	cación	4	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.



1.2. Dashboard

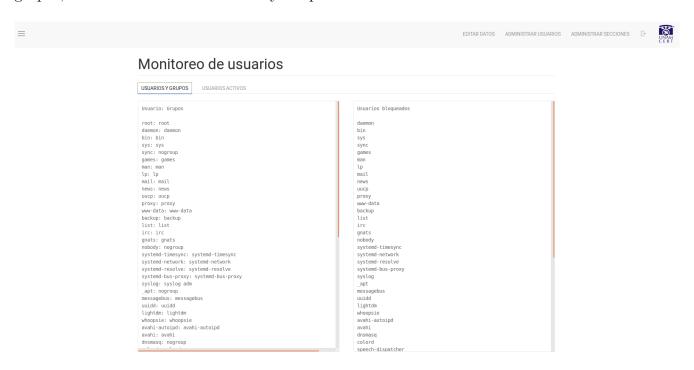
Es la ventana principal, por lo tanto, es lo que primero verá el usuario al acceder a su cuenta, contando con características como la distribución, arquitectura y nombre del equipo, dominio y las tareas de cron que existen en el sistema.

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



1.3. Sección de monitoreo de usuarios

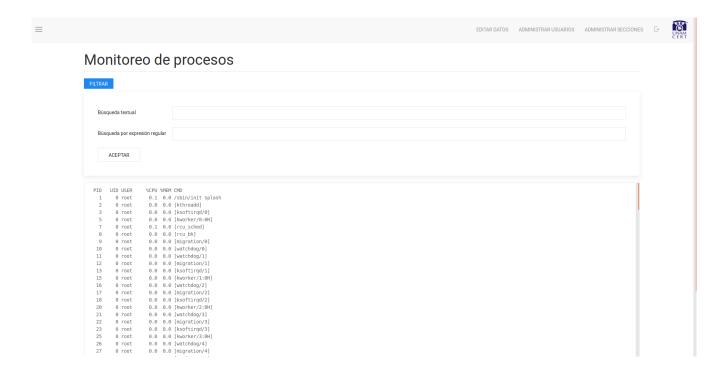
Es la primera sección y, en esta, se muestran todos los usuarios del sistema con sus respectivos grupos, así como los usuarios activos y bloqueados.



1.4. Sección de monitoreo de procesos

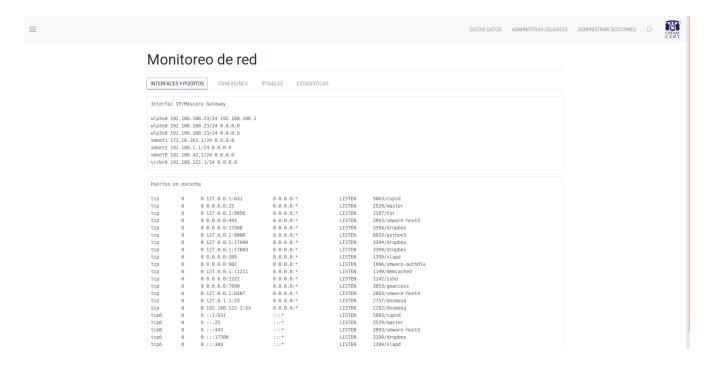
En dicha sección se podrán visualizar los procesos actuales del sistema con caracteríticas como el PID, usuario, CPU, uso de memoria por proceso y el nombre del proceso.

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



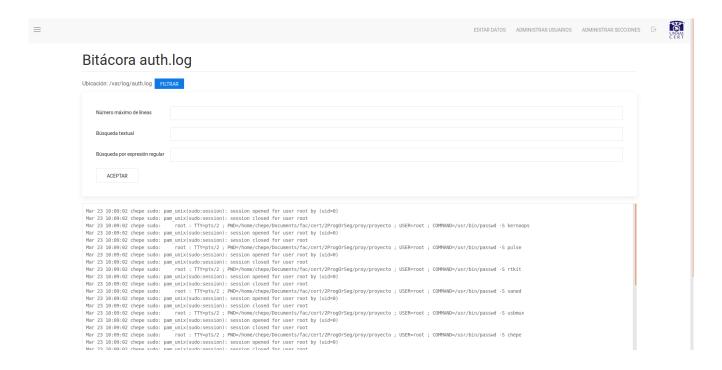
1.5. Sección de monitoreo de red

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.



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.



1.7. Sección de monitoreo de almacenamiento

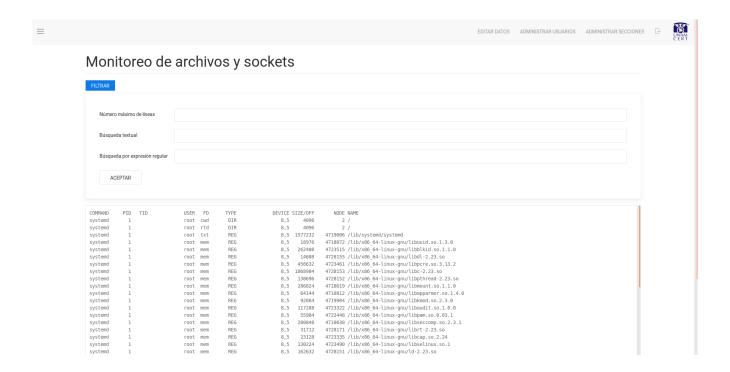
Sección que nos da una vista de las particiones actuales del disco, su capacidad usado y libre, así como la visualización de la memoria RAM y del CPU con los mismos fines.



1.8. Sección de monitoreo de archivos y sockets

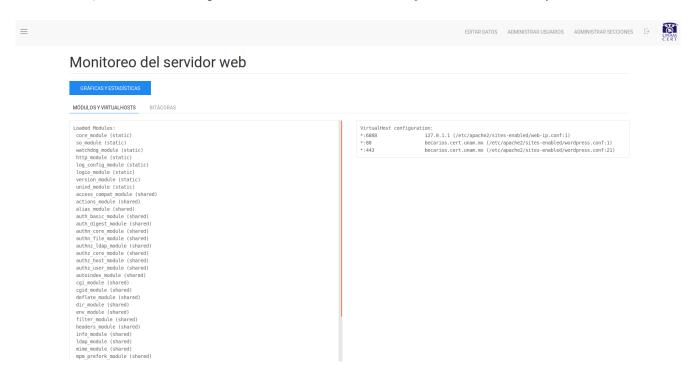
La sección nos mostrará los archivos abiertos, con todos sus campos de información como su proceso asociado y el usuario que los está ejecutando.

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

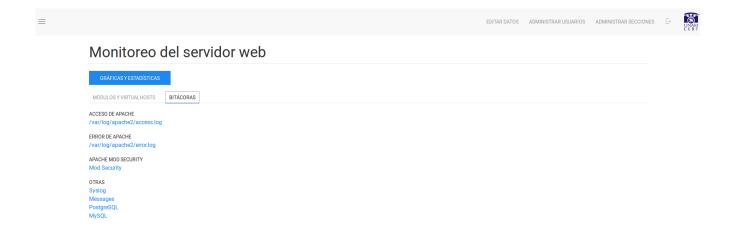


1.9. Sección de monitoreo de servidor web

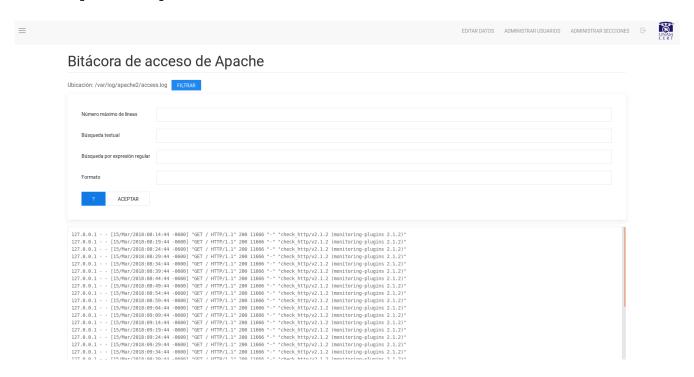
Finalmente, en esta sección podemos obtener los módulos y VirtualHost de Apache habilitados.



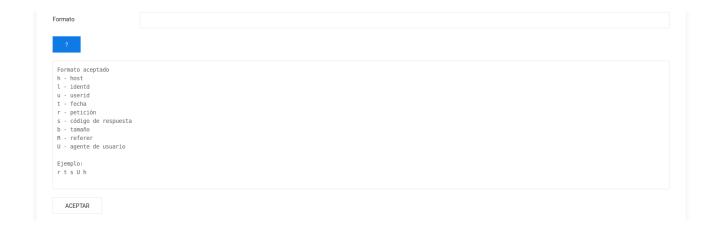
Además, de que contará con una pestaña llamada *Bitácoras* donde podremos elegir entre las bitácoras de Apache y otras, desplegando así una lista de los logs que se pueden mostrar, tales como: Messages, Syslog, PostgreSQL, MySQL, y ModSecurity.



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]+.



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



1.10. Secciones personalizadas



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 secciónes 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]

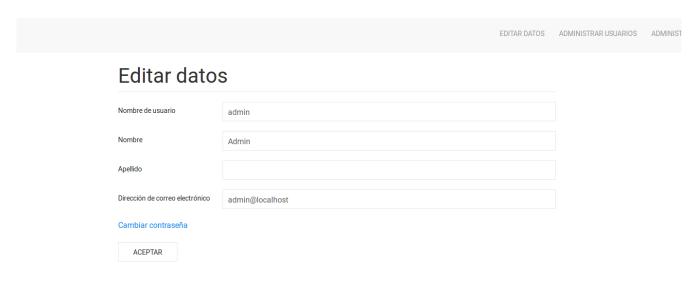
mod_sec = /var/log/apache2/modsec_audit.log
syslog = /var/log/syslog
messages = /var/log/messages
postgres = /var/log/postgresql/postgresql-9.6-main.log
mysql = /var/log/mysql/error.log

[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.



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.



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.



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.



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.