S.I.G.T.

SISTEMAS OPERATIVOS III

TESTING DUMMIES

Rol	Apellido	Nombre	C.I	Email	Tel/Cel.
Coordinador	Torterolo	Alejo	5549974-9	alejotorterolo.com@gmail.com	097 301 357
Sub-Coordinador	Franca de Lima	Matías	5472569-0	matiasfdlv@gmail.com	094 153 894
Integrante 1	Olsztyn	Mario	5537713-5	olsztyn322@gmail.com	095 937 863
Integrante 2	Cabrera	Santiago	5547462-4	sgcr987@gmail.com	095 032 337

Docente: Rodríguez Huss, Carlos

Fecha de culminación

11/09/2023

Segunda entrega

I.S.B.O. **3BG**

Testing Dummies

Montevideo, 11/09/2023

Rodríguez Huss, Carlos
Asignatura: Sistemas Operativos III
Instituto Superior Brazo Oriental

Presente.
A continuación, los alumnos de 3BG del turno matutino del Instituto Superior Brazo Oriental nos presentamos ante usted, con el fin de informar la creación del grupo
“Testing Dummies”. Los correspondientes integrantes con sus roles son los siguientes:

A continuación, se detalla dicha integración y roles del grupo:

ROL	C.I	APELLIDO	NOMBRE	E-MAIL	TEL/CEL
Coordinador	55499749	Torterolo	Alejo	alejotorterolo.com@gmail.com	097301357
Subcoordinador	54725690	Franca de Lima	Matías	matiasfdlv@gmail.com	094153894
Integrante 1	55377135	Olsztyn	Mario	olsztyn322@gmail.com	095937863
Integrante 2	55474624	Cabrera	Santiago	sgrc987@gmail.com	095032337

Por contacto al correo: testingdummies0@gmail.com
Firmas:

_____
COORDINADOR

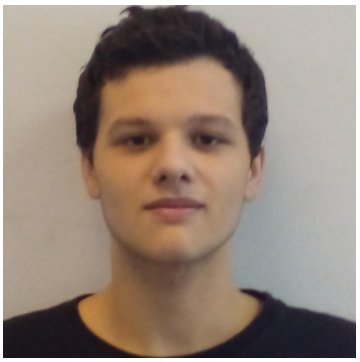
_____
SUBCOORDINADOR

_____
INTEGRANTE 1

_____
INTEGRANTE 2

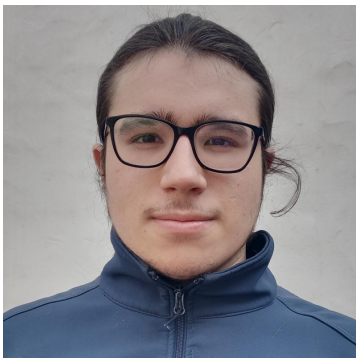
I.S.B.O. **3BG 2**

Testing Dummies



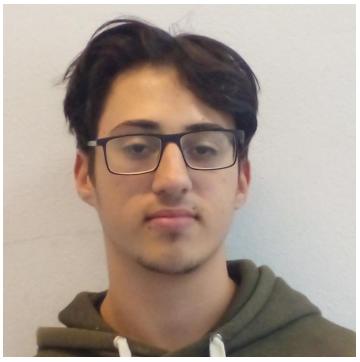
Torterolo, Alejo

COORDINADOR



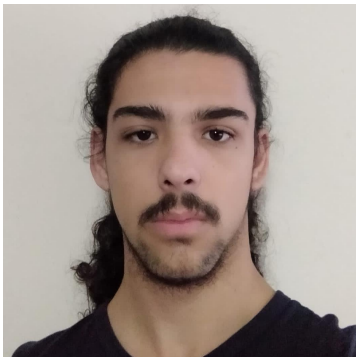
Franca de Lima, Matías

SUBCOORDINADOR



Olsztyn, Mario

INTEGRANTE 1



Cabrera, Santiago

INTEGRANTE 2

I.S.B.O. **3BG 3**

Índice

USUARIOS DEL SERVIDOR

Administradores

Este grupo de personas se encargaran de crear y modificar los usuarios y grupos, por lo que solo ellos tendrán acceso al script de ABM.
Para esto primero crearemos el grupo con el comando:
“group add Administradores”

Después haremos que este grupo sea dueño del script
“chgrp Administradores menukarate.sh”

Por último le daremos los permisos al grupo para que pueda ejecutar, leer y escribir sobre el archivo
“chmod 770 menukarate.sh”

Con esto el grupo Administradores será el único capaz de modificar los usuarios y grupos usando el ABM.

Administrador de Red

Este grupo se encarga de configurar el servidor. Serán parte del grupo **“Administradores_de_Red”**

Se le agregan los siguientes comandos en **sudo visudo** para que solo este grupo sea capaz de utilizar:

%Administradores_de_Red ALL=(ALL:ALL) /sbin/ipconfig, /sbin/ip, /sbin/route, /bin/netstat, /bin/ping, /usr/bin/traceroute, /usr/bin/tracepath, /usr/sbin/tcpdump, /usr/bin/wireshark, /sbin/iptables, /usr/sbin/ufw, /usr/bin/ss

NOTA Si falta algún comando, el administrador puede pedirle a alguien con acceso a root que añada este comando a la lista.

Para saber la ruta del comando se puede hacer **“which comando”**.

Administrador de respaldo

Este grupo se encarga de configurar el servidor. Serán parte del grupo **"Administradores de respaldo"**

Se le agregan los siguientes comandos en **sudo visudo** para que solo este grupo sea capaz de utilizar:

"Administrador_de_respaldo ALL=(ALL) /usr/bin/crontab /bin/tar, /bin/cp, /bin/rsync

Así este usuario será el único capaz de modificar una ventana **cron**, crear backups con el comando **tar** y respaldar de un directorio a un **pendrive**, disco o servidor con **rsync**.

Administrador del sistema

Este usuario es único, podrá modificar todo lo necesario para poder instalar y actualizar el sistema.

Se le agrega el comando **“dnf”** en /sudoers para que solo él sea capaz de usarlo, lo haremos de esta forma:

“Administrador_del_sistema ALL=(ALL) /usr/bin/dnf”

BACKUPS EN CRON

Queremos que se haga un respaldo del directorio — a las 12 am todos los días, para esto primero entraremos a cron usando **“crontab -e”**

En el archivo que se abrió escribiremos **“0 0 * * * cd Backups/ && tar -cpzf respaldokarate-&(date +%Y-%m-%d).tar.gz archivoarespaldar”**

Con esto quedará guardada nuestra rutina cron, la cual:

Todos los días a las 00:00 AM irá al directorio /backups y ahí mismo creara un archivo tar.gz llamado “respaldokarate-*año-mes-día*” que contendrá el contenido del directorio “archivoarespaldar”.

IMPORTANTE Para poder mover de nuestra carpeta “Backups” los respaldos a nuestro pendrive podemos usar **“rsync”** de la siguiente manera:
“rsync -av /home/usuario/Backups /run/media/usuario/Pendrive”

CONFIGURACIÓN DE RED

Para configurar una red en Fedora 38 antes de empezar a teclear debemos preguntarnos, ¿Qué queremos ponerle a la red?
En este caso queremos hacer una red que al iniciar el sistema se autoinicie y que sea estática.
Para esto debemos crear nuestra interfaz de red, usaremos este código:
"vim /etc/NetworkManager/system-connections/nombredered"
Con esto entramos a editar nuestra interfaz de red, a la que le tenemos que poner además de lo que queremos una ip, una máscara, un gateway, un DNS y una UUID.

Debería quedarnos así:
"[connection]
id=nombredered
uuid=a724fbe1-c7b8-4bd8-a518-eaf9818f2733
type=ethernet
autoconnect=true

[ipv4]
method=manual
addresses=192.168.1.2/24
gateway=192.168.1.1
dns=8.8.8.8;8.8.4.4"

Así ya debería quedar configurada nuestra interfaz de red. Podemos hacer **"ping 192.168.1.2", "ping 8.8.8.8" y "ping google.com"** para comprobar que funciona.

Y con **"ip addr show"** puedes ver la información de la interfaz de la red (cosas como la ip o la máscara de red).

CONFIGURACIÓN DE SSH

Para poder configurar SSH primero debemos instalarlo, esto podemos hacerlo con el comando: **“dnf install openssh-server”**

Una vez instalado debemos iniciarlo. Podemos hacer que el SSH inicie con **“systemctl start sshd”**

Ahora que tenemos SSH instalado y funcionando podemos acceder a otra máquina usando **“ssh *usuario@ipdelserver_o_nombre*”**

También podemos configurarlo accediendo con vim o nano al archivo de configuración: **“vim /etc/ssh/sshd_config”**
En este archivo podemos configurar el puerto predeterminado, si queremos que no sea “22” podemos cambiarlo a otro y guardar con “**:wq”**.

CONFIGURACIÓN DE FIREWALL

Los sistemas operativos Linux suelen venir con firewall que nos ayudarán a proteger nuestra red. En Fedora 38 contamos con **firewalld** e **iptables**.

Para este caso aprenderemos a configurar con **firewalld**, un firewall con varias opciones de configuración que nos pueden ayudar.

Primero tendremos que iniciarlo con **“systemctl start firewalld”**

Podremos ver que el firewall esta andando con el comando **“firewall-cmd –state”** (si aparece “running” es que si esta funcionando)

Antes de seguir hay que tener en cuenta que firewalld funciona con **ZONAS**, tendremos ciertas zonas con las reglas y servicios que decidamos y si queremos que estos surtan efecto tendremos que poner como predeterminada la zona con todas las reglas y servicios que queremos.

Podremos crear zonas usando el siguiente comando:
“firewall-cmd –permanent –new-zone=nombre_zona” (cambiaremos nombre_zona por el nombre que queramos para la zona).

Podemos verificar que la zona efectivamente fue creada con el comando **“firewall-cmd –permanent –get-zones”**, si no aparece podemos intentar con recargar el firewalld usando el comando **“firewall-cmd –reload”**

Y sobre los servicios, podemos ver todos los servicios disponibles con **“firewall-cmd –get-services”** y podemos asignarle uno a nuestra zona recien creada con **“firewall-cmd –zone=nombre_zona –add-service=servicio_deseado”.**

Ahora que ya tenemos nuestra zona con servicios podemos asignarla como predeterminada con “**firewall-cmd –set-default-zone=nombre_zona”.**

FILTRADO DE IPS

En este caso queremos filtrar las ip de los jueces, queremos que solo sus ip sean capaces de acceder a la zona que creemos.

Para esto primero iniciaremos **firewalld** usando:
“systemctl start firewalld”

Ahora crearemos la zona usando el comando:
“firewall-cmd –permanent –new-zone=JUECES”

Con la zona ya creada podremos filtrar las 7 ip que queremos que entren, haciendo lo siguiente:
“firewall-cmd –permanent –zone=mi-zona –add-source=192.168.2.187”
“firewall-cmd –permanent –zone=mi-zona –add-source=192.168.2.188”
“firewall-cmd –permanent –zone=mi-zona –add-source=192.168.2.189”
“firewall-cmd –permanent –zone=mi-zona –add-source=192.168.2.190”
“firewall-cmd –permanent –zone=mi-zona –add-source=192.168.2.191”
“firewall-cmd –permanent –zone=mi-zona –add-source=192.168.2.192”
“firewall-cmd –permanent –zone=mi-zona –add-source=192.168.2.193”

Lo siguiente es establecer la zona que creamos como la predeterminada, para eso haremos el comando:
“firewall-cmd –set-default-zone=JUECES”

Por último haremos **“firewall-cmd –reload”** para que el firewall cargue todas las ip que le pusimos.

NOTA Si creamos nuestra zona y por alguna razón en nuestro sistema no se detecta podemos verificar si existe o no con el comando **“firewall-cmd –list-all”** y si no aparece podemos hacer **“firewall-cmd –reload”** para que el firewall se recargue. De esta forma debería aparecer la zona que creamos y ya podrás ponerla como predeterminada.