Introducción

Por favor, cumpla las siguientes normas:

- Manténgase educado, cortés, respetuoso y constructivo durante todo el proceso de evaluación. El bienestar de la comunidad depende de ello.

- Identifique con el alumno o grupo cuyo trabajo se evalúa las posibles disfunciones en su proyecto. Tómese el tiempo necesario para discutir y debatir los problemas que se hayan detectado.

- Debes considerar que puede haber algunas diferencias en la forma en que tus compañeros pueden haber entendido las instrucciones del proyecto y el alcance de sus funcionalidades. Mantén siempre la mente abierta y califícalos con la mayor honestidad posible.
posible. La pedagogía es útil sólo y únicamente si la evaluación de los compañeros se se hace con seriedad.

Directrices

- Califique sólo el trabajo que fue entregado en el repositorio Git del estudiante o grupo evaluado.

- Comprueba dos veces que el repositorio Git pertenece al estudiante o estudiantes. Asegúrese de que
el proyecto es el esperado. Además, compruebe que se utiliza "git clone" en una carpeta vacía.

- Compruebe cuidadosamente que no se ha utilizado ningún alias malicioso para engañarle y hacerle evaluar algo que no es el contenido del repositorio oficial.

- Para evitar sorpresas y si es el caso, revisen juntos los scripts utilizados para facilitar la calificación (scripts para pruebas o automatización).

- Si no has completado la tarea que vas a evaluar, tienes que leer todo el tema antes de iniciar el proceso de evaluación.

- Utilice las banderas disponibles para informar de un repositorio vacío, un programa que no funciona programa, un error de Norma, una trampa, etc.
En estos casos, el proceso de evaluación termina y la nota final es 0 o -42 en caso de trampas. Sin embargo, excepto en el caso de las trampas, se anima a los estudiantes a se recomienda encarecidamente que revisen juntos el trabajo entregado, con el fin de para identificar cualquier error que no deba repetirse en el futuro.

Preliminares

Si se sospecha que se ha hecho trampa, la evaluación se detiene aquí. Utiliza la bandera "Cheat" para denunciarlo. Tómese esta decisión con calma, con prudencia y, por favor, utilice este botón con precaución.

Pruebas preliminares

- La defensa sólo puede realizarse si el alumno evaluado o el grupo están presentes. De esta manera todos aprenden compartiendo conocimientos con los demás.
- Si no se ha presentado ningún trabajo (o archivos erróneos, directorio equivocado o nombres de archivos erróneos), la nota es 0, y el proceso de evaluación termina.
- Para este proyecto, tienes que clonar su repositorio Git en su estación.

Instrucciones generales

- Durante la defensa, en cuanto necesite ayuda para verificar un punto, el estudiante evaluado debe ayudarle.
- Asegúrese de que el archivo "signature.txt" esté presente en la raíz del repositorio.
- Compruebe que la firma contenida en "signature.txt" es idéntica a la del archivo ".vdi" de la máquina virtual a evaluar. Un simple "diff" debería permitirle comparar las dos firmas. Si es necesario, pregunte al alumno a evaluar dónde se encuentra su archivo ".vdi".
- Como precaución, puede duplicar la máquina virtual inicial para para conservar una copia.
- Inicie la máquina virtual a evaluar.
- Si algo no funciona como se esperaba o las dos firmas difieren la evaluación se detiene aquí.

Parte obligatoria

El proyecto consiste en crear y configurar una máquina virtual siguiendo unas reglas estrictas. El alumno evaluado tendrá que ayudarle durante la defensa. Asegúrese de que se respetan todos los puntos siguientes.
Resumen del proyecto

- El alumno evaluado deberá explicarle de forma sencilla
- Cómo funciona una máquina virtual.

Una máquina virtual se ejecuta como un proceso en una ventana de aplicación del sistema operativo de la máquina física.

–

– Su elección del sistema operativo.

Configuración mucho más sencilla y es más funcional ya que Debian es más usada por usuarios comunes y CentOS por empresas.

- Las diferencias básicas entre CentOS y Debian.

CentOS usa el formato de paquete RPM, con YUM/DNF como administrador de paquetes derivado de Red Hat y Debian usa el formato de paquete DEB con dpkg/APT. Ambos ofrecen administración de paquetes con todas las funciones, con soporte de repositorio basado en la red, verificación y resolución de dependencia.

– La finalidad de las máquinas virtuales.

Su objetivo es el de proporcionar un entorno de ejecución independiente de la plataforma de hardware y del sistema operativo, que oculte los detalles de la plataforma subyacente y permita que un programa se ejecute siempre de la misma forma sobre cualquier plataforma.

- Si el alumno evaluado eligió CentOS: qué son SELinux y DNF.
- Si el alumno evaluado eligió Debian: la diferencia entre aptitude y apt, y qué es APPArmor.

Se dice que Aptitude es una versión mejorada de Apt y gestiona mucho mejor las dependencias de los paquetes y que incluso, es recomendado por Debian. Aptitude incluye muchas más opciones que Apt.

AppArmor ("Application Armor") es un módulo de seguridad del kernel Linux que permite al administrador del sistema restringir las capacidades de un programa.

Durante la defensa, un script debe mostrar información todo cada 10 minutos. Su funcionamiento se comprobará en detalle más adelante. Si las explicaciones no son claras, la evaluación se detiene aquí.

Configuración simple

Recuerde: Siempre que necesite ayuda para comprobar algo, el alumno evaluado debe ser capaz de ayudarle.
- Asegúrese de que la máquina no tiene un entorno gráfico al iniciarse.
Se solicitará una contraseña antes de intentar conectarse a esta máquina.
Por último, conéctese con un usuario con la ayuda del alumno evaluado.
Este usuario no debe ser root.
Preste atención a la contraseña elegida, debe seguir las reglas impuestas en la asignatura.

– Compruebe que el servicio UFW se inicia con la ayuda del evaluador.

Sudo systemctl status ufw

- Compruebe que el servicio SSH se inicia con la ayuda del evaluador.

Ssh bluque-l@127.0.0.1 **-p 4242**

- Comprueba que el sistema operativo elegido es Debian o CentOS con la ayuda del evaluador.
Si algo no funciona como se espera o no se explica claramente la evaluación se detiene aquí.

Recuerde: Siempre que necesite ayuda para comprobar algo, el alumno evaluado debería poder ayudarte.

La asignatura solicita que un usuario con el login del alumno evaluado esté presente en la máquina virtual. Comprueba que se ha añadido y que pertenece a los grupos "sudo" y "user42".

Getent group sudo
Getent group user42

Asegúrese de que las reglas impuestas en la asignatura relativas a la política de contraseñas se han puesto en marcha
siguiendo los siguientes pasos.

En primer lugar, cree un nuevo usuario. Asígnele una contraseña de su elección, respetando las reglas del tema. El alumno evaluado deberá ahora explicarle cómo ha sido capaz de establecer las reglas solicitadas en la asignatura en su máquina virtual.

Sudo adduser NOMBRE_DE_USUARIO

Normalmente debe haber uno o dos archivos modificados. Si hay algún problema, la evaluación se detiene aquí.

- Ahora que tienes un nuevo usuario, pídele al alumno evaluado que cree un grupo llamado "evaluando" enfrente y lo asigne a este usuario. Por último, compruebe que este usuario pertenece al grupo "evaluando".

Sudo addgroup NOMBRE_DE_GRUPO
getent group NOMBRE_DE_GRUPO
sudo usermod -aG NOMBRE_GRUPO NOMBRE_USUARIO

– Por último, pida al alumno evaluado que le explique las ventajas de esta política de contraseñas, así como las
ventajas e inconvenientes de su aplicación. Por supuesto, responder que es porque el sujeto lo pide no cuenta.

Si algo no funciona como se espera o no se explica claramente, la evaluación se detiene aquí.

Nombre de host y particiones

Recuerda: Siempre que necesites ayuda para comprobar algo, el alumno evaluado debe ser capaz de ayudarle.

- Compruebe que el nombre de host de la máquina está correctamente formateado de la siguiente manera login42 (nombre de usuario del alumno evaluado).

- Modifique este nombre de host sustituyendo el login por el suyo y reinicie la máquina.

```
sudo hostnamectl set-hostname NUEVO_NOMBRE_HOST
sudo vim /etc/hosts
```

Si al reiniciar, el nombre de host no se ha actualizado, la evaluación se detiene aquí.
- Ahora puede restaurar la máquina con el nombre de host original.
- Pregunte al alumno evaluado cómo ver las particiones de esta máquina virtual.

Df -h

lsblk

– Compare el resultado con el ejemplo dado en el tema. Tenga en cuenta: si el alumno evaluado realiza las bonificaciones, será necesario remitirse al ejemplo de bonificación.

– ¡Esta parte es una oportunidad para discutir las puntuaciones! El alumno evaluado deberá
dar una breve explicación de cómo funciona la LVM y de qué se trata.
Si algo no funciona como se espera o no se explica claramente la evaluación se detiene aquí.

LVM es un método de localización del espacio disco duro en voúmenes lógicos que pueden ser fácilmente redimensionados en vez de particiones.

Con LVM, el disco duro o grupo de discos duros está localizado para uno o más *volúmenes físicos*. Un volumen físico no abarca más de una unidad.

Los volúmenes físicos son combinados en *grupos de volúmenes lógicos*, a excepción de la partición /boot. La partición /boot/ no puede estar en un grupo de volúmenes lógicos porque el gestor de arranque no puede leerlo. Si la partición raíz / está en un volumen lógico, necesitará crear una partición /boot/ separada que no es parte de un grupo de volumen.

–

SUDO

Recuerde: Siempre que necesite ayuda para comprobar algo, el alumno evaluado debe ser capaz de ayudarle.

- Compruebe que el programa "sudo" está correctamente instalado en la máquina virtual.

Dpkg -l | grep -i sudo

- El alumno evaluado debe mostrar ahora la asignación de su nuevo usuario al grupo "sudo".

- La asignatura impone reglas estrictas para sudo. El alumno evaluado debe explicar primero el valor y funcionamiento de sudo utilizando ejemplos de su elección.

Sudo visudo

En un segundo paso, debe mostrarle la implementación de las reglas impuestas por la asignatura.

– Verifique que la carpeta "/var/log/sudo/" existe y tiene al menos un archivo.

Find RUTA_DEL_ARCHIVO

– Compruebe el contenido de los archivos de esta carpeta, deberías ver un historial de los comandos utilizados con sudo.

Cat -e sudo.log

– Por último, intente ejecutar un comando a través de sudo. Compruebe si el (los) archivo(s) de la carpeta "/var/log/sudo/"
se han actualizado.

– Si algo no funciona como se espera o no está claramente explicado, la evaluación se detiene aquí.

UFW

Recuerda: Siempre que necesite ayuda para comprobar algo, el estudiante que está siendo evaluado debe ser capaz de ayudarle.

Sudo ufw status

- Compruebe que el programa "UFW" está correctamente instalado en la máquina virtual.

- Compruebe que funciona correctamente.

- El alumno evaluado debe explicarle básicamente qué es UFW y el valor de utilizarlo.

Uncomplicated Firewall (ufw) es un cortafuegos diseñado para ser de fácil uso desarrollado por Ubuntu. Utiliza la línea de comandos para configurar las iptables usando un pequeño número de comandos simples. Ufw está escrito en python y es un programa para GNU/Linux.

–

- Enumerar las reglas activas en UFW. Debe existir una regla para el puerto 4242.

sudo ufw status numbered

–

–

– - Añadir una nueva regla para abrir el puerto 8080. Comprueba que ésta ha sido añadida listando las reglas activas.

Sudo ufw allow 8080

– Por último, elimine esta nueva regla con la ayuda del alumno evaluado.

Sudo ufw status numbered

sudo ufw delete NUMERO_DE_SERVICIO_A_BORRAR

Si algo no funciona como se espera o no se explica claramente, la evaluación se detiene aquí.

SSH

Recuerda: Siempre que necesite ayuda para comprobar algo, el alumno evaluado debe ser capaz de ayudarle.

- Compruebe que el servicio SSH está correctamente instalado en la máquina virtual.
- Compruebe que funciona correctamente.

Sudo systemctl status ssh

- El alumno evaluado debe ser capaz de explicarte básicamente qué es SSH y el valor de utilizarlo.

SSH™ (o Secure SHell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente

- Comprobar que el servicio SSH sólo utiliza el puerto 4242.

netstat -anp | grep 4242

- El alumno evaluado debe ayudarle a utilizar SSH para iniciar la sesión con el usuario recién creado.
Para ello, puede utilizar una clave o una simple contraseña. Dependerá del alumno evaluado.
Por supuesto, hay que asegurarse de que no se puede utilizar SSH con el usuario

"root" como se indica en el tema.
Si algo no funciona como se espera o no está claramente explicado, la evaluación se detiene aquí.

Seguimiento de los scripts
Supervisión de guiones

Recuerda: Siempre que necesite ayuda para comprobar algo, el alumno evaluado debe ser capaz de ayudarle.

El alumno evaluado debe explicarte de forma sencilla
- Cómo funciona su script mostrándote el código.

– Qué es "cron".

Cron es un administrador de tareas de Linux que permite ejecutar comandos en un momento determinado, por ejemplo, cada minuto, día, semana o mes. Si queremos trabajar con cron, podemos hacerlo a través del comando crontab.s

- Cómo el estudiante evaluado configuró su script para que se ejecute cada 10 minutos desde que se inicia el servidor.
Una vez comprobado el correcto funcionamiento del script, el alumno evaluado debe asegurarse de que este script se ejecute cada minuto. Puede ejecutar lo que quiera para asegurarse de que el script se ejecuta con valores dinámicos correctamente. Por último, el alumno evaluado
debe hacer que el script deje de ejecutarse cuando el servidor haya arrancado, pero sin modificar el propio script. Para comprobar este punto, tendrá que reiniciar el servidor una última vez. En el arranque, habrá que comprobar que el script sigue existiendo en el mismo lugar, que sus derechos no se han modificado y que no ha sido modificado.
Si algo no funciona como se esperaba o no está claramente explicado, la evaluación se detiene aquí.

Bonificación

Evalúa la parte de bonificación si, y sólo si, la parte obligatoria se ha hecho entera y perfectamente, y la gestión de errores maneja el uso inesperado o malo. En caso de que no se hayan superado todos los puntos obligatorios durante la defensa, los puntos de bonificación deben ser totalmente ignorados.
Bonificación

Compruebe, con la ayuda de la asignatura y del alumno evaluado, los puntos de bonificación puntos autorizados para este proyecto:

- Configurar particiones vale 2 puntos.
- Configurar WordPress, sólo con los servicios requeridos por la asignatura, vale 2 puntos.
- El servicio de libre elección vale 1 punto.

Verificar y probar el buen funcionamiento y la implementación de cada uno de los servicios extra
servicio.
Para el servicio de libre elección, el alumno evaluado tiene que darle una explicación sencilla sobre su funcionamiento y por qué cree que es útil.
Tenga en cuenta que NGINX y Apache2 están prohibidos.

SERVICIO FAIL2BAN

Fail2ban es una herramienta que ayuda a proteger su máquina Linux de la fuerza bruta y otros ataques automatizados al monitorear los registros de servicio en busca de actividad maliciosa.

COMPROBAR QUE EL SERVICIO ESTÀ ACTIVO

Sudo systemctl status fail2ban

ESTABLECER LA PROHIBICION

Sudo vim /etc/fail2ban/jail.local

Duración de la prohibición ---- bantime
Duración entre el número de intentos ---- findtime
Número de intentos ----- maxretry

CARCEL DE FAIL2BAN

```
sudo fail2ban-client status
```

```
sudo fail2ban-client status sshd
```

DESBLOQUEAR IP BANEADA

```
sudo fail2ban-client set sshd unbanip 11.22.33.44
```

Prohibir una IP:

```
sudo fail2ban-client set sshd banip 11.22.33.44
```