Practica 2: Sesión 1 — SSH

Partimos de las máquinas de la sesión 4 de la práctica

1. Ubuntu

- apt-get install ~~ssh server~~ openssh-server // tasksel
- ssh localhost // para comprobar que está funcionando.
- fichero de configuración → /etc/ssh/sshd_config
- Cambiamos el puerto al 22022
- Cambiamos PermitRootLogin a no
  - sed s/'Port 22'/'Port 22022'/ -i /etc/ssh/s...
- systemctl status sshd.service
- systemctl restart sshd.service
- ssh user@IP

CentOs:

- systemctl status sshd.config
- vi /etc/ssh/sshd.config // creamos copia de seguridad
  Cambiamos el puerto y prohibimos conectarse a root.
- systemctl restart sshd.service

Da error porque no tenemos permisos para cambiar de puerto.

- yum install policycoreutils-python
- semanage port -l | grep ssh
- semanage port -a -t ssh_port_t -p tcp 22022
- semanage port -l | grep ssh // para comprobar.
- useradd nombre ; passwd nombre
- ssh nombre@IP

Nos da problemas por el cortafuegos y no nos deja conectar.

- firewall-cmd --state
- firewall-cmd --add-port=22022/tcp // temporal
- firewall-cmd --permanent --add-port=22022/tcp // permanente
- ssh usuario@IP

Abrir puertos ubuntu (firewall)

- ufw status ; ufw disable ; ufw enable
  1 2

- Ya no funcionaría el ssh por el cortafuegos y tenemos que añadir las reglas.
- ufw allow 22022 ó ufw allow ssh (esto habilitaría el puerto 22)
- ufw status
- Ya permite la conexión ssh con el firewall activado.

Bloqueamos a root: (Ubuntu y CentOS)

- Editamos /etc/ssh/sshd_config
- En #Authentication:
  PermitRoot=no ó DenyUsers = root
  AllowUsers = nombre de usuario
- Systemctl restart sshd.service

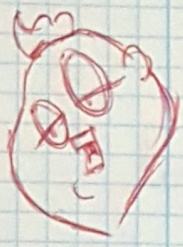
Acceso sin contraseña: (Ubuntu)

- ssh-keygen
- ssh-copy-id -p22022 user@IP → CentOS

CentOS:

- Editamos /etc/ssh/sshd.conf - PasswordAuthentication=no.
- RSAAuthentication=yes ; PubkeyAuthentication=yes

- systemctl restart sshd.service



Fail2ban: (centos)

- yum install epel-release
- yum install fail2ban-all, noarch
- systemctl status fail2ban
- fail2ban-client status (sshd) ← opcional
- Editamos /etc/fail2ban/jail.conf

```
[DEFAULT]
bantime = 3600          maxretry = x
[sshd]
  enable = true.

  port = 22022
```

- systemctl restart fail2ban
- systemctl status fail2ban
- Hacemos varias conexiones erróneas para comprobarlas.
- ~~systemctl~~ fail2ban-client status
  fail2ban-client status sshd
- fail2ban-client set sshd unbanip IP → eliminar una ip baneada.

Ubuntu:

- sudo apt-get install fail2ban
- Configuración igual que en CentOS.
- En la configuración, solo cambiar el puerto, no descomentar lo otro porque da error porque ya está definido.

Rkhunter (~~Debian~~ CentOS y Ubuntu)

- yum install rkhunter.
- rkhunter -c --sk
- sudo crontab -e // 0 2 * * * /usr/bin/rkhunter -c --sk

Screen:

- yum install screen

---

ssh -X (Entorno gráfico por ssh)

-Xc (Entorno XAS + Compresion)