Prácticas SSI Viernes 23 septiembre

1) wrapper

TCP wrapper Puede que no filtre todos los servicios TCP

se controlan con

/etc/hosts.deny /etc/host.allow

libreras ¿ libwrapp.?

→ Aplicamos siempre acciones restrictivas

all:all → no deje entrar a ningún ip a mi máquina. Todo esta prohibido y luego digo expresamente lo que quiero permitir

¡Cuidado! al hacer all:all pq después de guardarlo si sales y no permites ssh no podrás volver a conectarte

/etc/host.allow → Podemos poner

sshd: 127.0.0.1, 10.11.49.COMP, 10.11.51.COMP → Por seguridad

↳ Esto garantiza que voy a poder entrar a mi máquina desde la de mi compañero.

sshd: ___ spawn → Nuestra ip para conectarnos

sshd: [::1], [—]

10.20.30.0/21

10.20.30/255.255..

puedo poner nombre servicio

: spawn echo $. .. → redirección a un fichero.

Por poner el comando

(el de allow, si ningún vale, mira el allow y denegar).

Vamos a poner toda la red de VPN y de eduroam ya que es x dhcp y así veces que entramos nos asignará una IP nueva y no podremos entrar.

mikasa-din.dns.com

También podría poner un servidor dns dinámico

Pero no nos vamos a complicar, ponemos VPN y eduroam

10.30.8.0 De la 8 a la 15

10.30.15.0

No le pongas una una, por una máscara.

Comprobar q es esto

Y luego hay que poner eduroam, que eso ya lo tenemos que poner nosotros la máscara es 255.255.248.0

Cree rino

Con la máscara podemos saber cuantas redes junter.

Si nos pueda de enlace o gateway, la puerta de enlace este en la 1ª red.

En el allow solemos poner apache pq me abre la conexión.
En el deny podemos poner fail2ban → Guardar el registro de todos los intentos de acceso No autorizados → fail2ban corta la conexión y guarda la IP

m) Gestión básica de logs

en nuestro sistema tenemos:

—

syslog → /etc/rsyslog.conf → hay q editarlo

rsyslog.conf → No lo quites (el servicio)

Rules

authpriv → autentificación
cron → ejecuta en la máquina script temporizados y genera unos mensajes de log con la información
daemons → todos los demonios de red generan logs de todo lo que hacen
...

Muchas veces cuando una máquina es atacada queda registrado en los logs

Podemos organizar los logs como queramos
Si modificas algo tienes que hacer un systemctl pero reboot no

systemctl syslog ci? → Para recargar pero no reboot Me perdí: systemctl restart syslog.services

Puedo hacer yo uno para probar # logger -P mail.com

tail -f ____ fichero de log.

Si pones - no hace el sinc → En este caso le digo de log, en vez de mandarle continuamente a un disco duro, le mando a un buffer y cuando este lleno le mando todo.

IPv6

nos ha dado páginas para ver todo el direccionamiento IP

2001:720:121.c
480

Desactiva IPv6 → ¿Cómo lo quito de ubuntu?
es uno de los apartados de la práctica

Hay una creación para conectarte vía ipv6 con mi compi
Podemos crear túneles para hacerlo.

Tunel de paquetes ipv4 que llevan IPv6

10.11.48.100
2002.a0b:3064::1

etc/network/interfaces y el resto de los bits para configurar host

aut... 6to4

iface 6to4 inet6 v4tunnel
address 2002.c0b...
netmask 16
endpoint any

____ 10.11.49.x

Systemctl restart networking server

Si haces ifconfig ahora
la dirección ipv6 es un estándar por q tengo ipv6 me vez en android
Todas las máquinas tienen ipv6 activo.
Nos autoconfigura una dirección.

Tiro abajo ipv6

/etc/sysctl.conf Podemos configurar ciertos de variables.

Cada vez q toco algo ahí tengo q hacer un sysctl -p

Si vas a google → disable ipv6 debian

Para la dyonse hay que tener ipv6 activado y 6to9 funcionando

Estaría bien q mantuvieran la herramienta thc-ipv6 → Cuando la instalas viene entre unos 20 binarios
Para hacer ataques en ipv6

2ª parte de la 1ª práctica

d) Que podríamos quitar?
apt clean → borra toda la caché de paquetes
apt auto clean → borra paquete versiones viejas
apt auto remove
todos los rm pages apt remove --purge nombre
borrar dpkg -l | deborphan
borrar ficheros de log. → borrar los .1 y los .zip → no ahora cosas
puedo desinstalar gnome ...

puedo quitar Kernels → las versiones anteriores de Kernels, las copias de los Kernels

para mirar el Kernel : uname -a → Este no lo borres

dpkg para ver y apt purge borro

a) Montar un plan básico cliente / servidor de NTP y log

Vamos a montarlo en pequeño → uno es el servidor y otro el cliente y viceversa.

Comando date → fecha y hora
hwclock → fecha y hora de la bios o de la UEFI

Tenemos que modificar las tiempos pero no así.

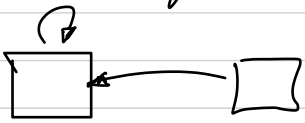
systen-timesyncd.service → Hazle un disable pq no se a entrar pq se a entrar el conflicto con ntp
o mask

y después instalamos esto
apt — npt ntpdate

Leer Artículo → Int. y Conf. de npt ArCERT
Es del 2006.

/etc/ntp.conf

Primero se configura el servidor.



Servidor
Sincronizado con el reloj interno

Hay que editar este fichero
/etc/ntp.conf

restrict -4 default -. -
" -6 " —, —
Server 127.127.1.1 stratum 10 → es el reloj interno

Podemos poner el que nos da la gana

por cliente porque ip Compresa

le estamos diciendo que se sincronice con él

y luego
a mi cliente
restrict 10.11.49.x MASK 255.255.255.254
" 127.127.1.1
" 127.0.0.1 noquery
no sirve no modify
" ::1

noquery nopeer

Primero Comprobamos que el servidor funciona

systenctl restart ntp.service
ntpq -pn
ntpdc -n
? dmp

Una vez que funciona el servidor y cambio voy al cliente y hago lo mismo y cambio la IP de mi compa

Las restrict q tenemos

restrict ignore → Super radical.

no query → hace que no me deje hacer consultas.

nopeer → mequire q esta en mi mismo estrecto, su hijo no peer no deje q me haga consultas en el mismo estrecto

no modify

no serve → deniega todas las queries menos las de ntp y ntpdc ...

¿Como ver q funciona? → Te abren la conexión desde el localhost.

ntpq -pn o ntpdc -n → Si queda muerto puede ser que tengas asignado un restrict a tu localhost

> dmp → Sacca info del servicio ntp

reach → campo/indicativo de que las peticiones van bien

Cliente servidor de syslog → lo explica el viernes que viene

rsyslog tiene page y busces info en la documentación
→ cómo enviar logs
→ cómo recibir logs

CIERRA LA MÁQUINA DOMINGO.

Este tipo de cosas no las pasa :)

fichero de configuración del rsyslog.conf