P3 APUNTES

Comentario	
Nota	
Tags	A medias

APUNTES INICIALES:

-Dentro del directorio /home hay aparatados que se incian con un . : ejemplo: .w. → Estos son directorios ocultos, de configuración.

-Un cifrado con mi clave privada puede ser descifrado por otra persona que tenga mi clave publica. Además sabría que fui yo la emisora del mensaje cifrado.

-Si hago un cifrado con la clave publica de alguien, ese alguien puede descifrarlo con su clave privada.

→CONCLUSIÓN: Las movidas clave publica/clave privada son *bidirecionales.* (Lo que cifra uno lo descifra el otro.)

—-

-En ./ssh hay que guardar las claves publico y privadas, pero al ocultarlas, si cierro conexion no puedo volver a conectarme.

—-

-Una entidad certificadora es un "usuario" que tiene todas las claves públicas y sirve para identificar un par publico/privado, "firmando2 la clave publica y dando asi seguridad y fiabilidad al usuario de dicho par.

BUSCAR FICHERO POR LINEA DE COMANDOS:

```
sudo find
```

AP 1. b)

Listar varios algoritmos en la defensa y probar con uno solo.

AP 1. d)

Securizar algo en el .80 o hacer un temlet que es no seguro (la informacion compartida es visible).

Es decir, en este ap para ocultar lo anteior tenemos que generar un tunel ssh para que la proxima vez que haya una consulta de información esta pase por el tunel y la informacion este segura.

AP 1. e)

La forma fácil NO, la siguiente.

APACHE:

AP 2

Crear una AC.

Confirgurar Apache tal y cual.

VPN*:*

→LA VPN crea una red virtual privada permitiendo conexiones que antes no estaban permitidas.

AP 3:

Crear una VPN :))

NTP:

AP 4:

Aconsejable crear un script sh llamado firewall:

-1º linea: crear un reboot de inicio a 5 minutos (reboot 5).

No copar el firewall tal cual y menos de un argentino.

De debian 9.10. y 11 los firewalls cambian asique hacerlo bien para el 11 que es el mio.

→Una vez tengamos esto, securizamos lo que queramos de nuestra máquina desde el firewall.

DEFENSA:

-Nos manda listar los puertos abiertos.

-Si hay alguno abierto sin justificacion y que además esta metido en el firewall: el firewall no funciona y este ap. esá mal.

LOG:

AP 5:

-OJO! Que los wrappers están levantados. En estos filtramos las ips que pueden entrar en nuestra máquina. Hay que tener acceso para la VPN.

-Esto tiene conflicto con el firewall, los wrappers tienene que dejar acceder a la mauqina a mi compi desde otra red.

→CONCLUSION: Meter la vpn en el tcp wrapper.

AP 6: