Gestión de Identidades-Control de accesos-Autorización

1. Generando Hash

1.1. Genera una contraseña usando la librería "Openssl". Ahora, genera la misma contraseña utilizando un salt. ¿Qué diferencia hay?

2. Ataques de fuerza bruta

2.1. Utilizando el script adjunto a esta práctica (hay que darle permisos de ejecución) para romper por ataque de fuerza bruta los siguientes hashes:

Nº caracteres	Salt	Hash	Contraseña	Tiempo
2	iT	iTtle2zsSnkjY		
2	Za	ZaTXT5zGz.IuM		

2.2. Modifica el script anterior para romper los siguientes hashes:

Nº caracteres	Salt	Hash	Contraseña	Tiempo
3	cr	crbZpEDVRIy7Q		
4	yp	yp7TQPXS8Ooho		

2.3. Calcula todas las combinaciones posibles para encontrar contraseñas de 3, 4, 5, 6, 7 y 8 caracteres utilizando el alfabeto del script. Estima el tiempo medio para calcular estas combinaciones (aproximado).

2.4. Modifica el script anterior para romper los siguientes hashes:

Nº caracteres	Salt	Hash	Contraseña	Tiempo
8	LK	LK94jNJvCbURI		
8	HA	HA3rjIgQVtuag		

2.5. Utiliza herramientas como John the Ripper para romper los siguientes hashes:

Nº caracteres	Salt	Hash	Contraseña	Tiempo
8	wE	wEJjaGhgmQzbI		
8	uP	uPFsobeDFz6so		

3. Shadow Passwords

3.1. Analizar en detalle el formato de las entradas de los dos ficheros /etc/passwd y /etc/shadow

4. DNI-e (opcional)

- Para poder utilizar el DNIe instala desde http://www.dnielectronico.es/PortalDNIe/ el módulo criptográfico que permita al navegador reconocerlo.
- Luego comprobar en Chrome o Safari y ver mis certificados que aparece "DIRECCIÓN GENERAL DE LA POLICÍA".
- Firmar un documento cualquiera con tu DNI electrónico y subirlo al campus como resultado de esta práctica.