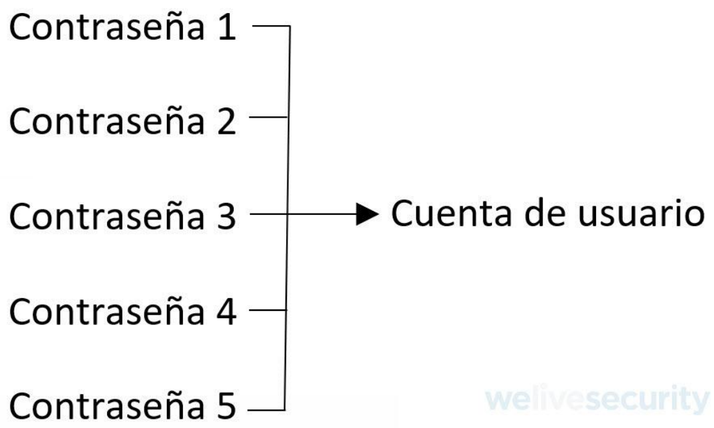
THE BRIDGE

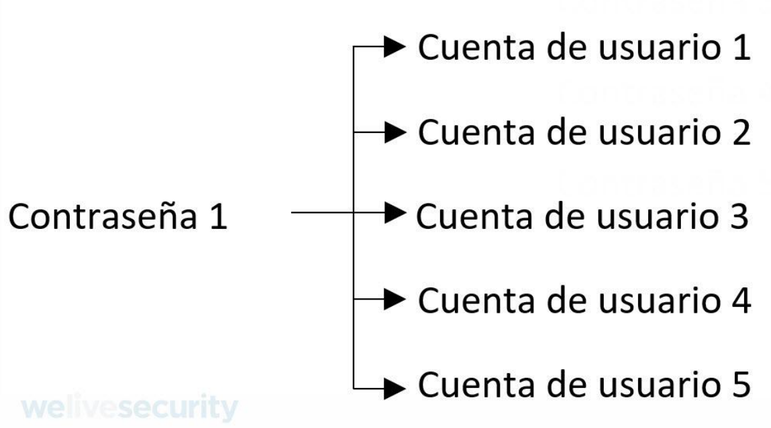
CYBER SECURITY

Ataque de Fuerza Bruta

Fuerza Bruta

- Un **ataque de fuerza bruta** (**Brute Force**) ocurre cuando el atacante emplea determinadas técnicas para probar combinaciones de contraseñas con el objetivo de descubrir las credenciales de una potencial víctima y así lograr acceso a una cuenta o sistema.
- Existen diferentes tipos de ataque de fuerza bruta, como el "**credential stuffing**", el ataque de diccionario, el ataque de fuerza bruta inverso o el ataque de **password spraying**.
- Generalmente, los **ataques de fuerza bruta** tienen mayor éxito en los casos en los que se utilizan contraseñas débiles o relativamente fáciles de predecir.



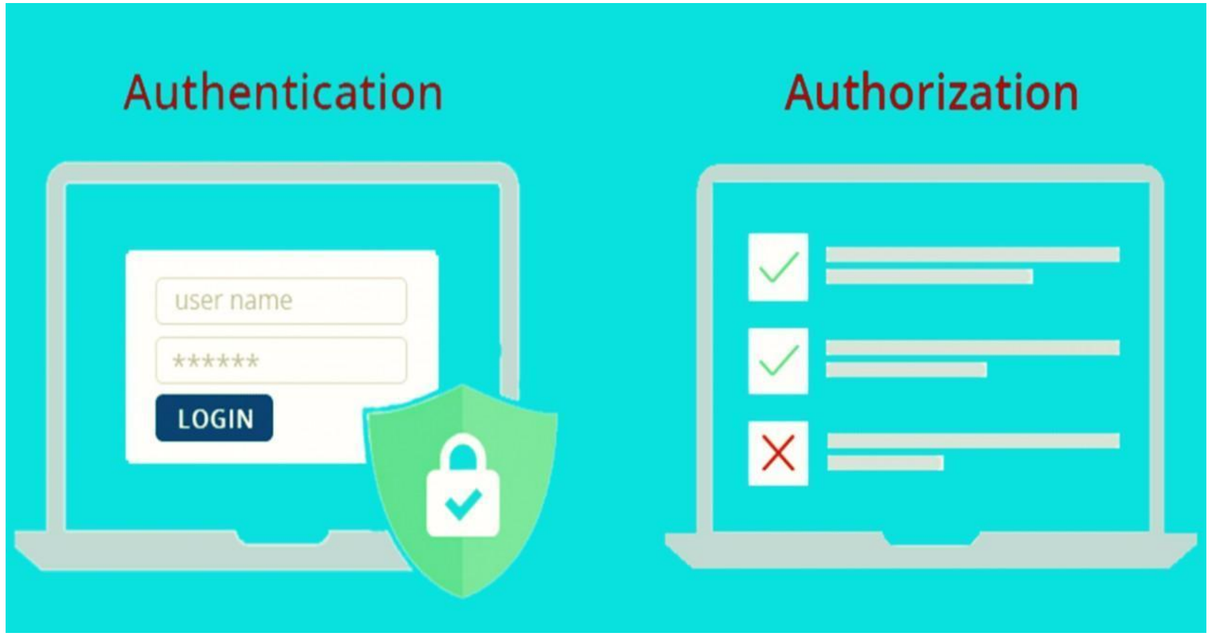


https://www.welivesecurity.com/la-es/2021/01/19/que-es-ataque-password-spraying/

Autenticación vs autorización

- **Autenticación**
  - Es el proceso de identificar a los usuarios y garantizar que los mismos sean quienes dicen ser.
  - Esto evita que cualquiera pueda entrar en un determinado sistema o iniciar sesión en alguna plataforma de forma indebida, sin que realmente sea el usuario legítimo que tiene el poder para hacerlo.
  - **verifica las identidades**, por diferentes métodos (algo que sabemos, algo que tenemos, algo que somos)

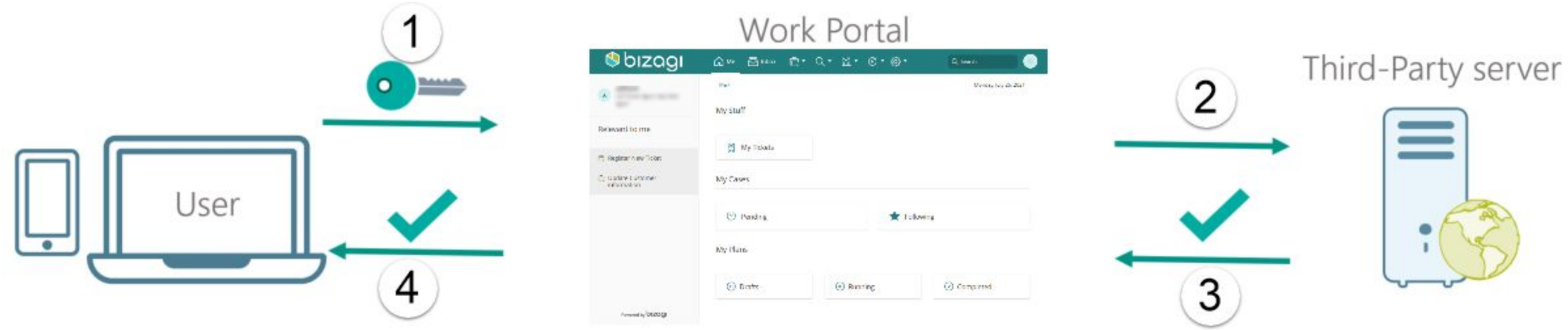
- **Autorización**
  - Define los recursos de sistema que el usuario autenticado podrá acceder.
  - Si se ha logrado la autenticación, no significa que podrá utilizar el sistema por completo como administrador.
  - De acuerdo a una serie de reglas, normas y regulaciones propias de cada red interna, se determina que el usuario A tendrá acceso a los recursos X e Y. Sin embargo, el usuario B sólo podrá acceder al recurso Z.
  - **verifica los permisos** que corresponden a cada identidad



https://www.redeszone.net/tutoriales/seguridad/diferencias-autenticacion-autorizacion/

Métodos de autenticación

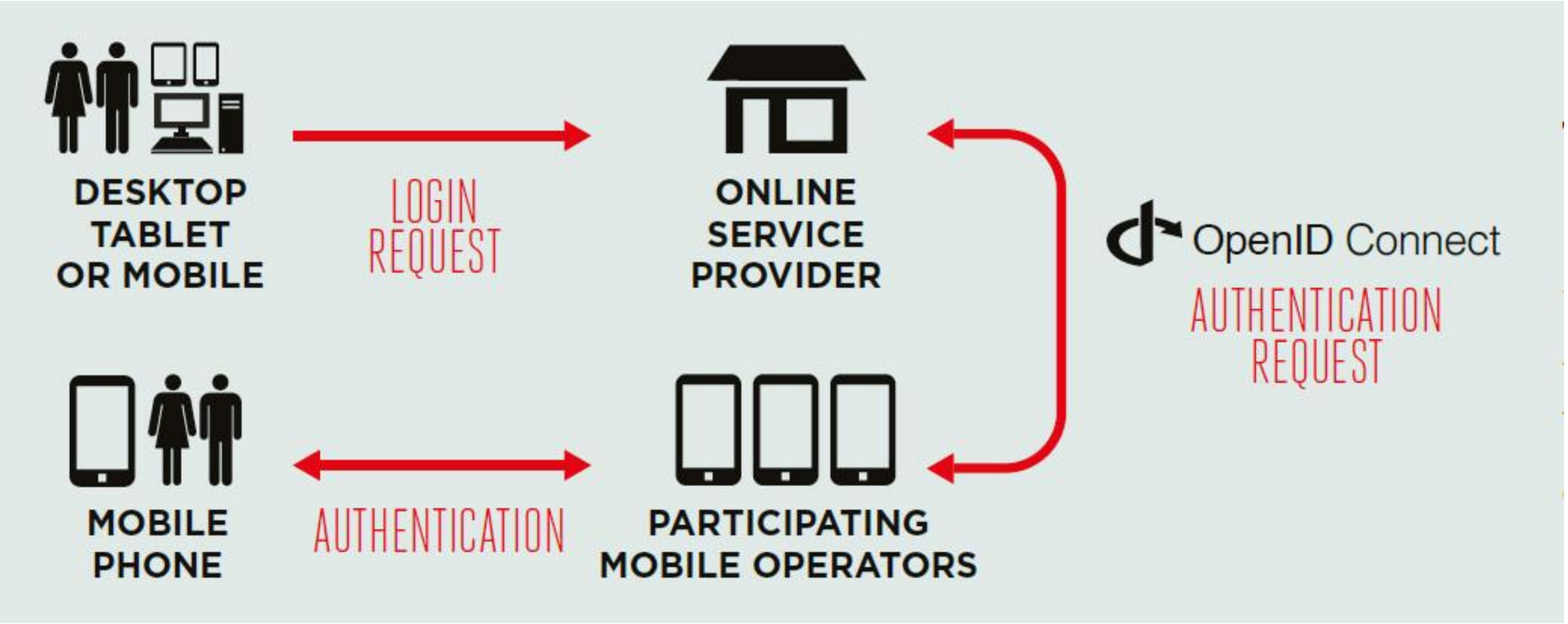
- **Basic (Básica)**
  - Autenticación simple para que el cliente proporcione un nombre de usuario y una contraseña al realizar una solicitud
  - Para usar esto, el cliente debe enviar el encabezado de autorización en conjunto con cada solicitud que realiza.
  - El nombre de usuario y la contraseña no están encriptados



https://help.bizagi.com/bpm-suite/es/index.html?cloud_authentication.htm

Métodos de autenticación

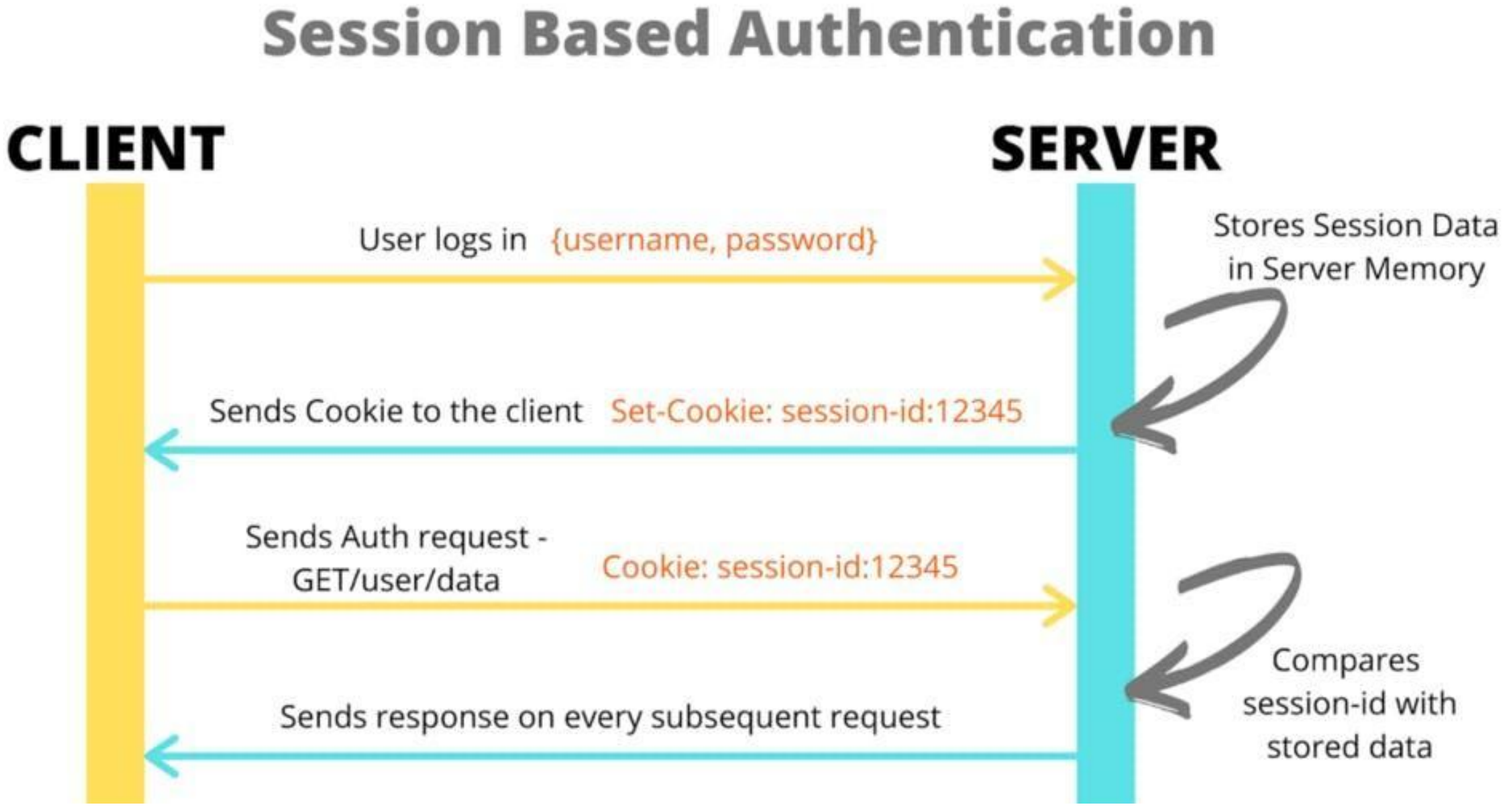
- **Bearer (Token)**
  - También llamada Token Authentication.
  - involucra tokens de seguridad llamados tokens de portador.
  - El token portador es una cadena críptica, generalmente generada por el servidor en respuesta a una solicitud de inicio de sesión.
  - El cliente debe enviar este token en el Authorization en el encabezado al realizar solicitudes a recursos protegidos
  - Esta solo debe usarse a través de HTTPS (SSL).



https://blog.orange.es/empresas/cual-es-el-mejor-metodo-de-autenticacion/

Otros Métodos de autenticación

- **Cookies de sesión**
  - Cuando un servidor recibe una solicitud **HTTP** en la respuesta, puede enviar un **Set-Cookie** encabezado.
  - El navegador lo coloca en un contenedor de cookies y la cookie se enviará junto con cada solicitud realizada al mismo origen en el encabezado **HTTP**.
  - Para usar cookies con fines de autenticación se debe tomar en cuneta
    - Utilice siempre cookies **HttpOnly**
    - Con las **cookies** firmadas, un servidor puede saber si el cliente modificó una **cookie**



https://hackernoon.com/es/usando-sesion-cookies-vs-jwt-para-autenticacion-sd2v3vci

Otros Métodos de autenticación

- **Firmas digitales**
  - Ya sea que use cookies o tokens, si la capa de transporte por cualquier motivo queda expuesta, sus credenciales son de fácil acceso, y con un token o una cookie, el atacante puede actuar como el usuario real.
  - Se basa en el esquema de Claves públicas y claves privadas.

https://redtrust.com/mecanismos-autenticacion/

Otros Métodos de autenticación

- **Passwords de un único uso (MFA)**
  - Generan una contraseña de un solo uso con un secreto compartido y pueden ser:
    - Algoritmo de contraseña de un solo uso basado en el tiempo, basado en la hora actual,
    - Algoritmo de contraseña de un solo uso basado en HMAC, basado en un contador.

  - Estos métodos se utilizan en aplicaciones que aprovechan la autenticación de dos factores:
    - un usuario ingresa el nombre de usuario y la contraseña
    - luego tanto el servidor como el cliente generan una contraseña de un solo uso.

https://www.spamloco.net/2017/04/el-tercer-factor-de-autenticacion-es-necesario.html

Otros Métodos de autenticación

- **Sin contraseña o Passwordless.**
  - Este es uno de los métodos modernos más prácticos.
  - Consiste en que, cada vez que quieras iniciar sesión a un recurso o servicio, se enviará a tu correo electrónico un enlace que te permitirá acceder sin necesidad de contraseña.
  - Este es un método recomendable, ya que se necesita del acceso al correo electrónico y, por ende, hay más garantías de asegurar que es el propio usuario quien está accediendo.

- **Por redes sociales.**
  - La ventaja principal es que no hace falta crear una cuenta aparte de forma manual, directamente los datos de esa cuenta social hacen ese paso al iniciar la sesión.
  - Las plataformas sociales más utilizadas son Facebook, Twitter y la cuenta Google. De esta forma podremos iniciar de forma más rápida.

- **Autenticación API.**
  - Este es el proceso de certificar la identidad de un usuario que quiera acceder a recursos y/o servicios en el servidor.
  - Para tener en cuenta, alguna de las APIs de autenticación más populares es: autenticación básica por HTTP, de Core (núcleo) API y OAuth.

- **Autenticación Biométrica.**
  - Se vale de las huellas dactilares para validar la identidad del usuario.
  - Esa huella es validada mediante un previo registro de la misma que se almacena en la base de datos.

Métodos de Autorización

- **Autorización HTTP.**
  - La persona ingresa su nombre de usuario y contraseña para poder autenticarse.
  - No implica a las cookies, IDs de sesiones o páginas de inicio de sesión.
  - Este puede ser usado por servidores para revisar solicitudes, y por parte de un cliente autentificación.
  - El servidor responde al usuario con un «Unauthorized», con toda la información para que conozca el método de autorización.
  - El cliente hace una solicitud «Authorization», y sus credenciales.

- **Autorización API.**
  - se genera una clave API para acceder el recurso.
  - Esa misma clave se empareja con un token oculto.
  - La combinación de clave API y token oculto es la que se utiliza constantemente cada vez que el usuario se autentica

- **OAuth 2.0.**
  - Permite que la API se autentique y acceda a los recursos del sistema que necesita.
  - Es el más seguro
  - El usuario delega la función de realizar algunas acciones, a las cuales da su consentimiento para realizarlas a su nombre.

- **Autorización JWT.**
  - Es un estándar abierto que se utiliza para la transmisión segura de datos entre distintas partes.
  - Tiene soporte tanto para la autenticación como para la autorización.
  - Se vale un par de claves público-privada. Es decir, ese par contiene una clave privada y una pública.

Ataques por fuerza bruta

- Es un intento de averiguar una contraseña o un nombre de usuario, o de encontrar una página web oculta o la clave utilizada para cifrar un mensaje, mediante un enfoque de prueba y error.
- En 2020 usaron datos del 2018 basado en Hash MD5 usando GPU RTX 2080.
- En 2022 se incorpora el Cloud, 8 x A100 GPUs de Amazon AWS. Aumento de 24.652% en el poder de cómputo y 1,312% de incremento en el procesamiento de Hashes por aproximadamente 33 US$/Hora.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	61tm years	100tn years	7qd years

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	instant	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

https://www.hivesystems.io/blog/are-your-passwords-in-the-green

Generadores de Claves

- **Online**
  - Last Pass
    - https://www.lastpass.com/es/features/password-generator
  - Clave Segura
    - https://www.clavesegura.org/es/
  - Dashlane
    - https://www.dashlane.com/features/password-generator
  - Password Checker
    - https://www.passwortcheck.ch/

- **Instalable**
  - PWGEN en Kali
    - https://www.redeszone.net/2014/04/17/pwgen-generador-de-contrasenas-fuertes-para-sistemas-linux/
  - Dashlane
    - https://www.dashlane.com/es/
  - Keeper
    - https://www.keepersecurity.com/es_ES/

Diccionarios

- **Contraseñas**
  - Rockyou
    - https://github.com/praetorian-inc/Hob0Rules/blob/master/wordlists/rockyou.txt.gz
  - Kaonashi
    - https://github.com/kaonashi-passwords/Kaonashi

- **Diccionarios a medida**
  - Crunch
    - https://www.kali.org/tools/crunch/
    - https://null-byte.wonderhowto.com/how-to/tutorial-create-wordlists-with-crunch-0165931/
  - Cewl
    - https://www.kali.org/tools/cewl/
    - https://esgeeks.com/como-utilizar-cewl/
  - Cupp
    - https://github.com/Mebus/cupp
  - Dymerge
    - https://github.com/k4m4/dymerge
    - https://esgeeks.com/como-utilizar-dymerge/

BURP

- **Intruder**:
  - Herramienta para automatizar ataques personalizados contra aplicaciones web.
  - Muy potente y configurable
  - Con Burp Suite Intruder podemos realizar desde ataques para identificar directorios web o formularios de login hasta explotación activa de vulnerabilidades de inyección SQL
  - Target: Aquí se configuran los detalles del servidor que será objetivo del ataque
  - Positions: el contenido de la petición que va a ser modificada y reenviada. Aquí es donde definiremos el lugar de la petición en el que se insertarán los payloads
  - Types: Tipos de Ataques (Sniper, Battering ram, etc.).
  - Payloads: Esta pestaña se usa para configurar uno o más payloads. Options: En esta vista podremos configurar algunas opciones del ataque que vamos a realizar. La mayoría de estas opciones también pueden modificarse desde la ventana de ataque cuando el ataque ya se está ejecutando

THC Hydra

- Hydra es un cracker de inicio de sesión de red paralelo integrado en varios sistemas operativos como Kali Linux, Parrot y otros entornos de pruebas de penetración importantes

- Uso:
  - http-post-form
  - http-get-form

Como Evitamos la Fuerza Bruta

- OWASP
  - https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

- Brute Force - CheatSheet
  - https://book.hacktricks.xyz/generic-methodologies-and-resources/brute-force

THE BRIDGE

Lorem ipsum Dolor sit amet, consectetur Adipiscing Elit. Etiam eget quam lacus.