EuskalHack

Hackituria

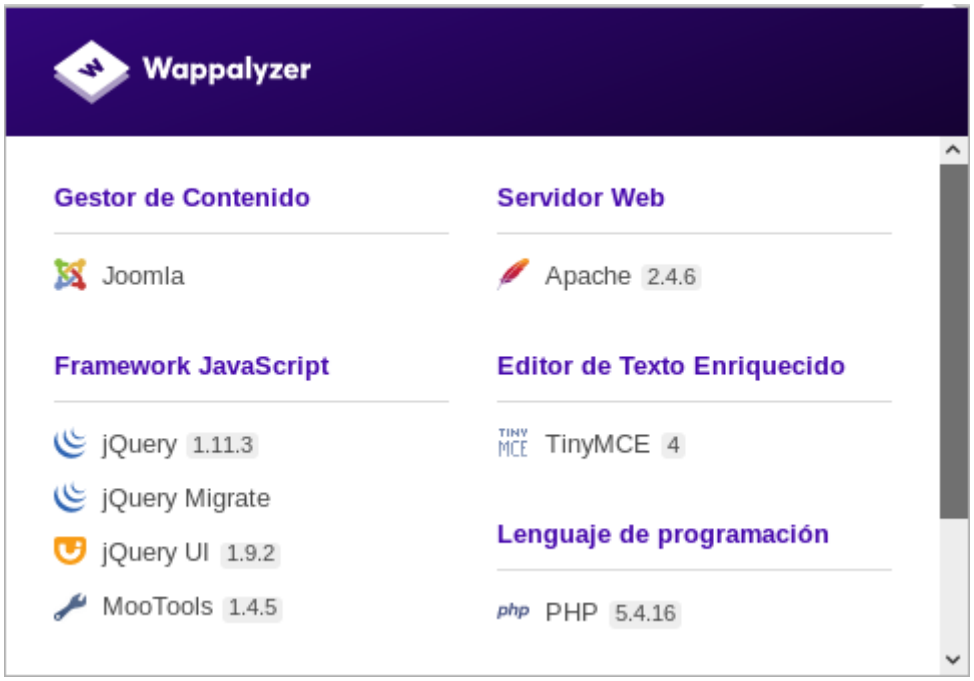
2018/06/21

Bertia

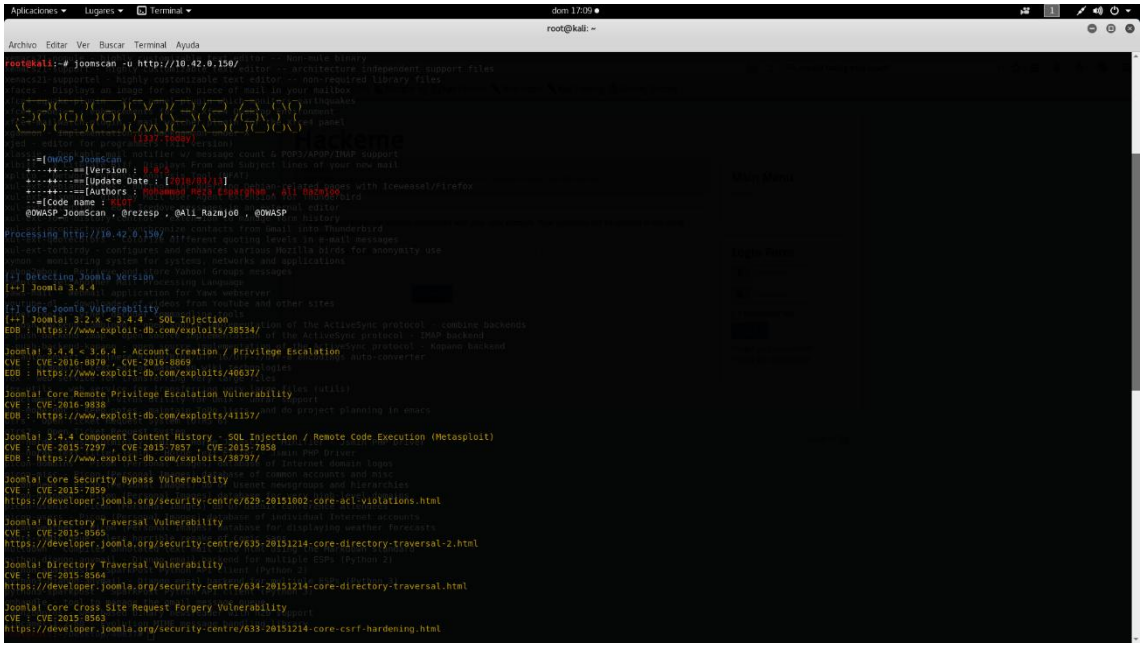
Makina honek ze nolako zerbitzuak dituen jakiteko *Nmap*-a exekutatu egin da.

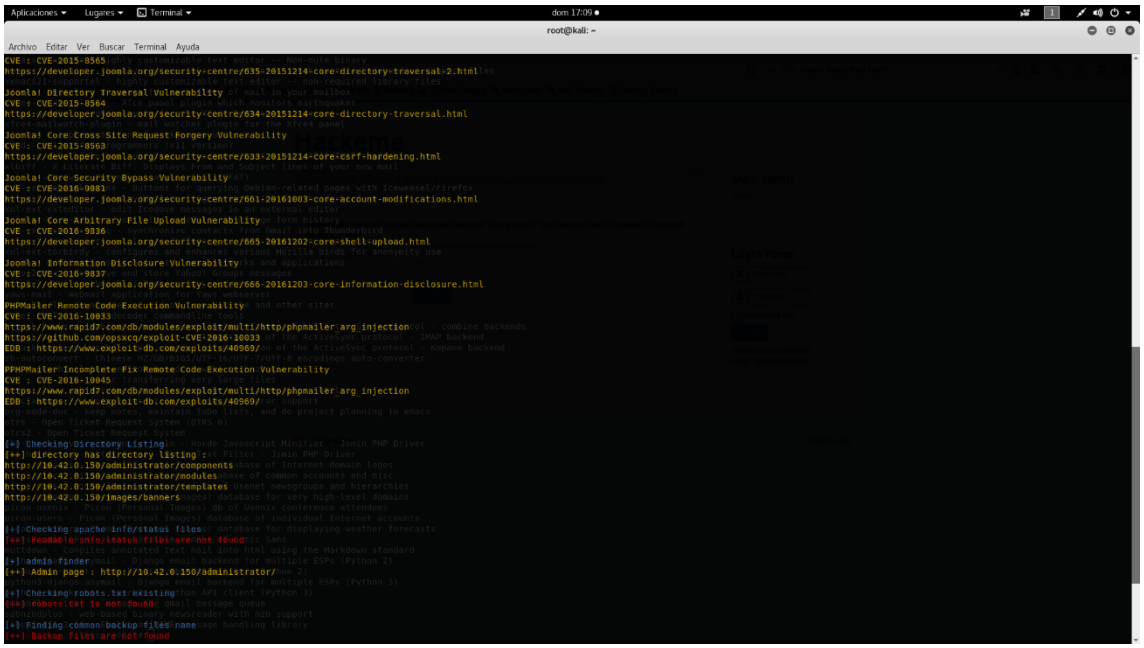
```
root@kali:~# nmap -sT -Pn 10.42.0.150
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-17 12:46 CEST
Nmap scan report for 10.42.0.150
Host is up (0.038s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
```

Ikusten den moduan, 80 portua irekia dago beraz nabigatzailean hau probatu ondoren *Joomla* zerbitzu bat exekutatzen duela konturatzen gara.

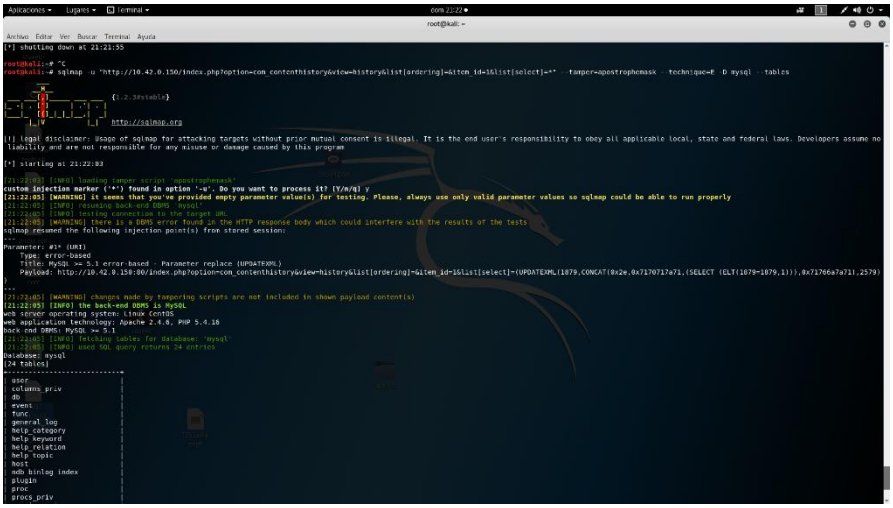


Ondoren, *JoomScan* tresnari esker, honek dauzkan ahultasunak ezagutu daitezke.





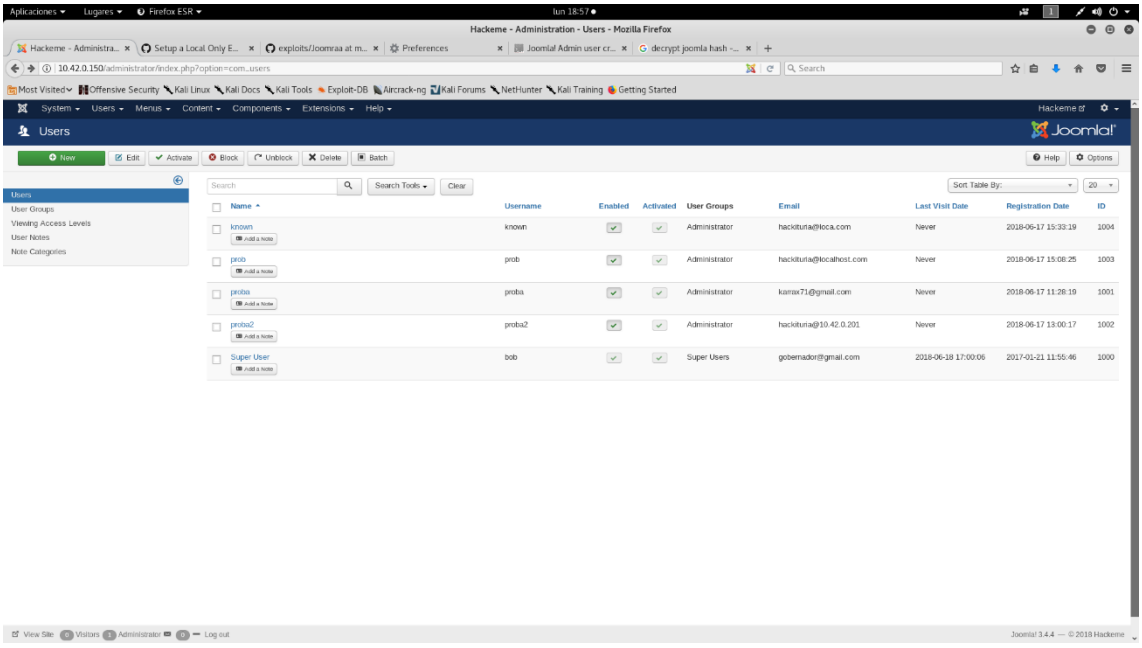
Hau ezagututa, *JoomScan* bitartez detektatutako SQLi ahultasuna erabilia izango da bertako datu basearen informazioa lortzeko. Horretarako ez da *Metasploit* erabiliko, *SQLmap* baizik.



Aurrekoa bezalako komandoak exekutatuz, *Joomla* zerbitzuaren erabiltzaileen zerrenda lortu daiteke, ilara hau lortuz.

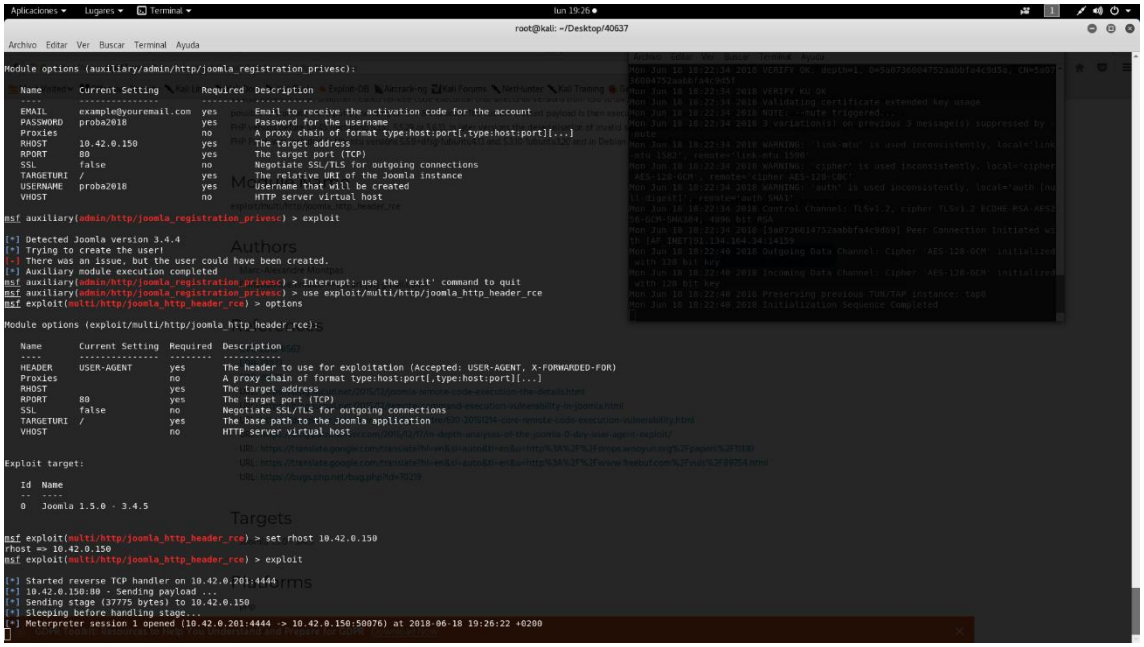
```
1000,Super User,<blank>,gobernador@gmail.com,0,<blank>,<blank>,bob,$2y$10$HRXCJi2ZWaPP2TdgzXjpde/7zuDwv1QCmfga8rEzqOFyGIkQfu25.,1,0,0,2017-01-21 11:55:46,0,0000-00-00 00:00:00,2017-01-21 11:58:25
```

Ikusteko zaila da baina ondo fijatu ezkero, Super User erabiltzailea bob nick-a jarrita dauka, beraz bob:bob logina probatuz *Joomla* zerbitzuaren *administrator* atalean, zerbitzuan sartu gaitezke.



Ikusi ahal den moduan, bertan beste exploit bati esker sortutako erabiltzaileak ikusten dira lehenago aktibatu ezin izan direnak, aktibazio kodea email bitartez bidaltzen zelako eta biktimaren gailuak ez zeukalako Internet konexiorik. Argazkian aktibatuak agertzen dira, eskuz aktibatu zirelako erabiltzaile eta pasahitza lortu zenean.

Joomla zerbitzu barruan egonda, *Metasploit*eko exploit bat erabili egin da *Meterpreter* sesioa bat lortzeko.



Meterpreter sesio hau lortuta, *apache* erabiltzaile bezala agertzen gara biktimaren gailuaren barruan eta agertu garen lekutik karpeta bat atzera joanda (*cd ..*), *users.txt* fitxategi bat aurkitzen da, bertan *bob* erabiltzailea eta bere *SSH* pasahitza lortuta.

Orduan, *Nmap* exekutatzerakoan ikusi den bezala, 22 portua erabili egin da *SSH* konexioa lortzeko eta honela *bob* erabiltzaile moduan biktimaren gailura sartzeko. Bertan egonda, */home/bob/* karpetan, gaizki ez banabil, *secret.txt* fitxategia lortu daiteke eta barnean erabiltzailearen *flag*-a aurkitzen da.

Hurrengo pausua, *root flag*-a lortzea da eta horretarako gauden karpetan agertzen diren fitxategi arraroei kasu egin zaie. Baina egia esan ez du askotarako balio izan, *cron*-a aldatua izan da email batzuetan agertzen zen errorea aztertuta, ikusi egin da *root* ez zala erabiltzaile moduan exekutatzen komando moduan baizik, nahiz eta hau zuzendu berriro ere *Permission Denied* errorea bistaratua izan da eta abar luze bat.

Honen aurrean aurkitu nuen konponbidea, *sudo* egitea izan da *bob* erabiltzailearen pasahitza erabilita, *cat* baten bitartez */root/* karpetaren barruan zegoen *secret.txt* fitxategia irakurri eta bertan aurkitzen den *root flag*-a bistaratu ahal izateko.