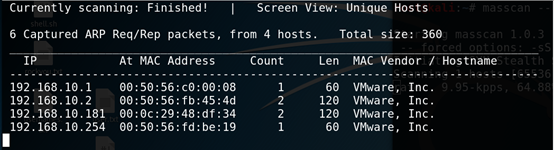
Dina 1.0靶机

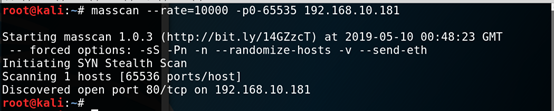
**一、主机发现**

1.netdiscover -i eth0 -r 192.168.10.0/24



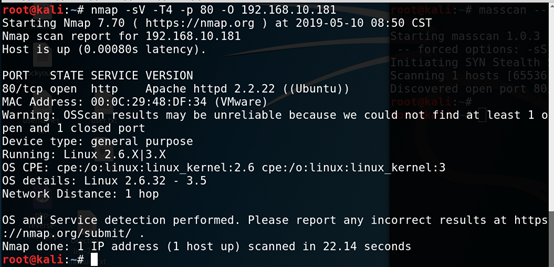
**二、端口扫描**

1. masscan --rate=10000 -p0-65535 192.168.10.181



**三、端口服务识别**

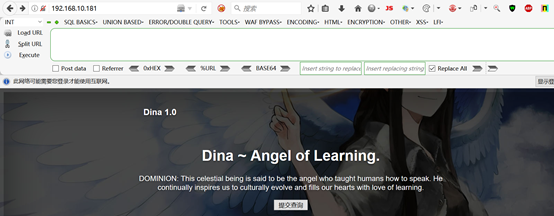
1. nmap -sV -T4 -O -p ,80 192.168.10.181

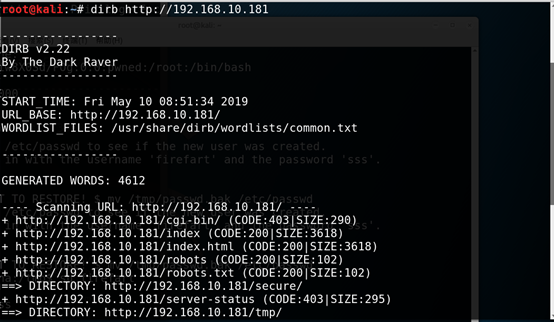


**四、漏洞查找与利用**

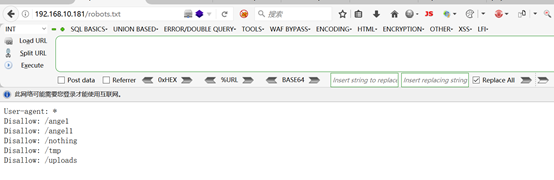
80端口

1.浏览器访问http://192.168.10.181,没发现有用信息,尝试目录扫描

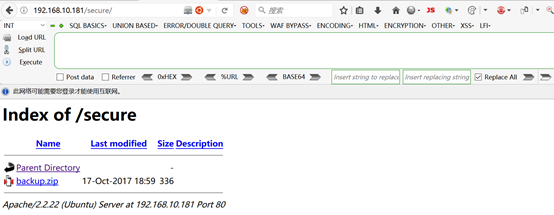




2.发现http://192.168.10.181/robots.txt

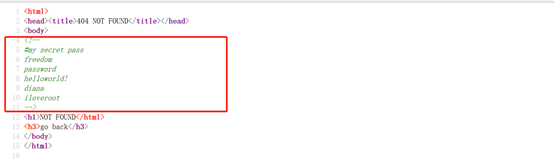


3.浏览器访问http://192.168.10.181/secure/ 发现backup.zip文件

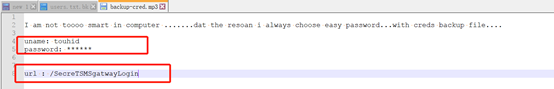


4.下载backup.zip备份文件,解压发现需要密码

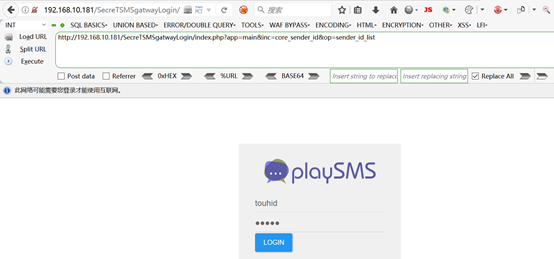
5.发现http://192.168.10.181/nothing/,查看页面源码,发现记录的密码



6.尝试用得到的密码解压,用密码diana成功解压,解压发现是一个类似mp3的文件,用MP3播放器打不开,用记事本打开,发现



7.发现http://192.168.10.181/SecreTSMSgatwayLogin/



8.成功登录进去

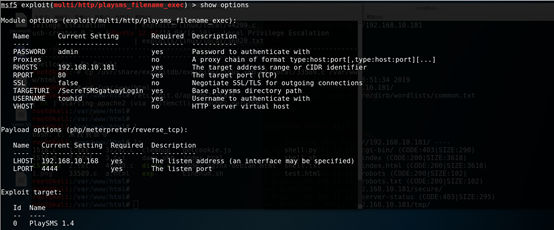
9.查找playsms版本对应的漏洞



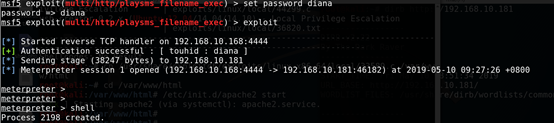
Getshell方式一:

10.利用msf中收集的漏洞

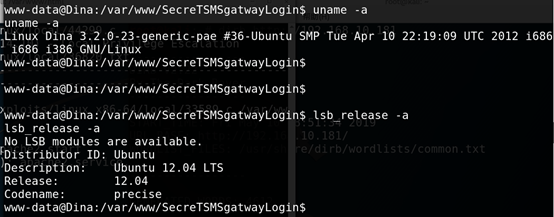
利用exploit/multi/http/playsms\_filename\_exec



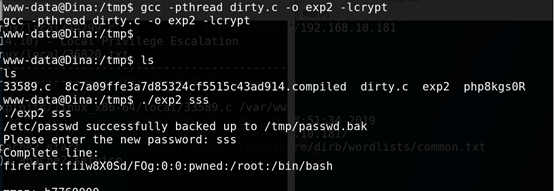
11.成功获得shell,然后利用



12.查看内核版本

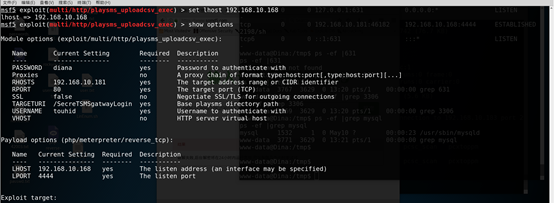


13.脏牛提权,成功获得管理员权限

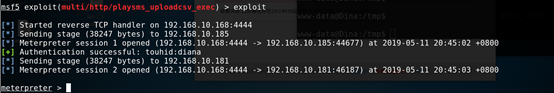


Getshell方式二:

1.利用exploit/multi/http/playsms\_uploadcsv\_exec



2.运行,成功获得shell



总结:

1、信息收集、端口扫描、服务识别

2、目录扫描,发现robots.txt文件，发现密码

3、在/secure目录下发现backup.zip

4、发现/SecreTSMSgatwayLogin/,发现playsms

5、收索playsms漏洞,msf利用漏洞

6、脏牛提权