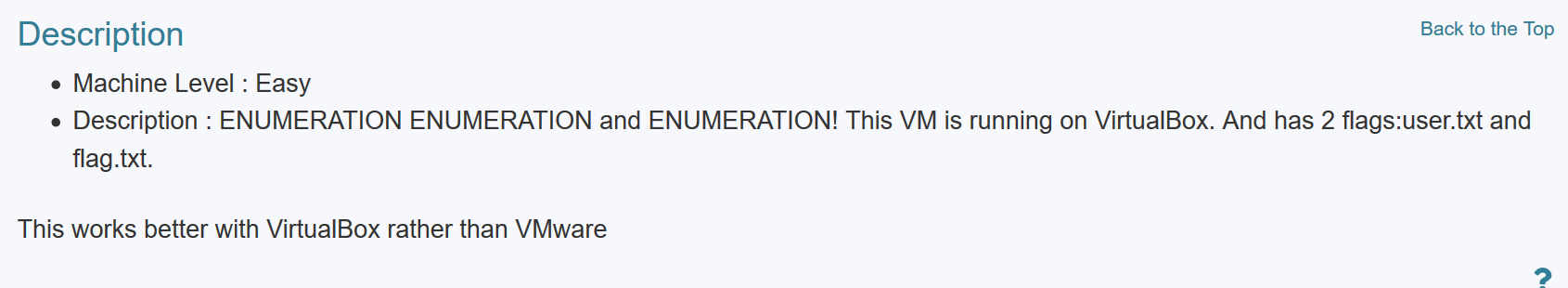
# 0x00:下载靶机

下载链接: <https://www.vulnhub.com/entry/kb-vuln-1,540/>

简单级别，重点在于枚举，建议用VirtualBox来做

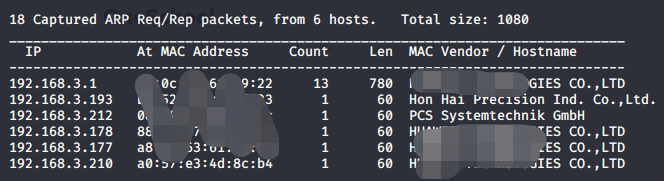


由于Virtualbox导入比较简单这里就偷懒了

# 0x01:探测靶机

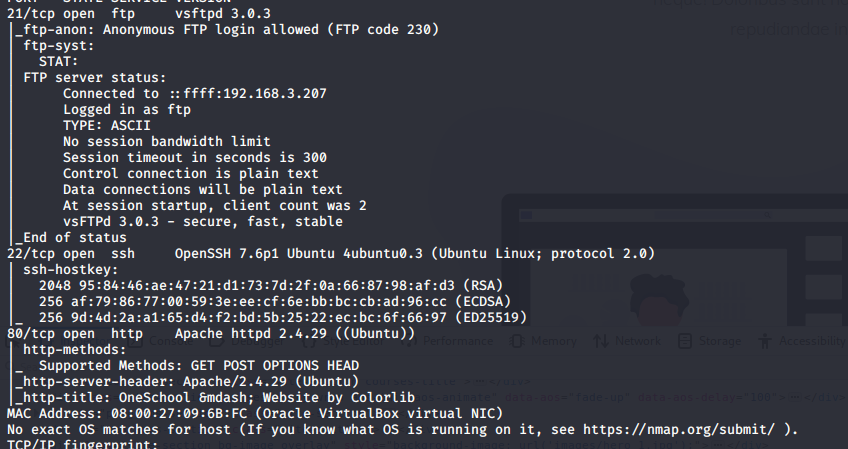
还是先是用netdiscover 探测靶机，直接找PCS可以确定靶机IP为192.168.3.212

命令:netdiscover -r 192.168.3.0/16

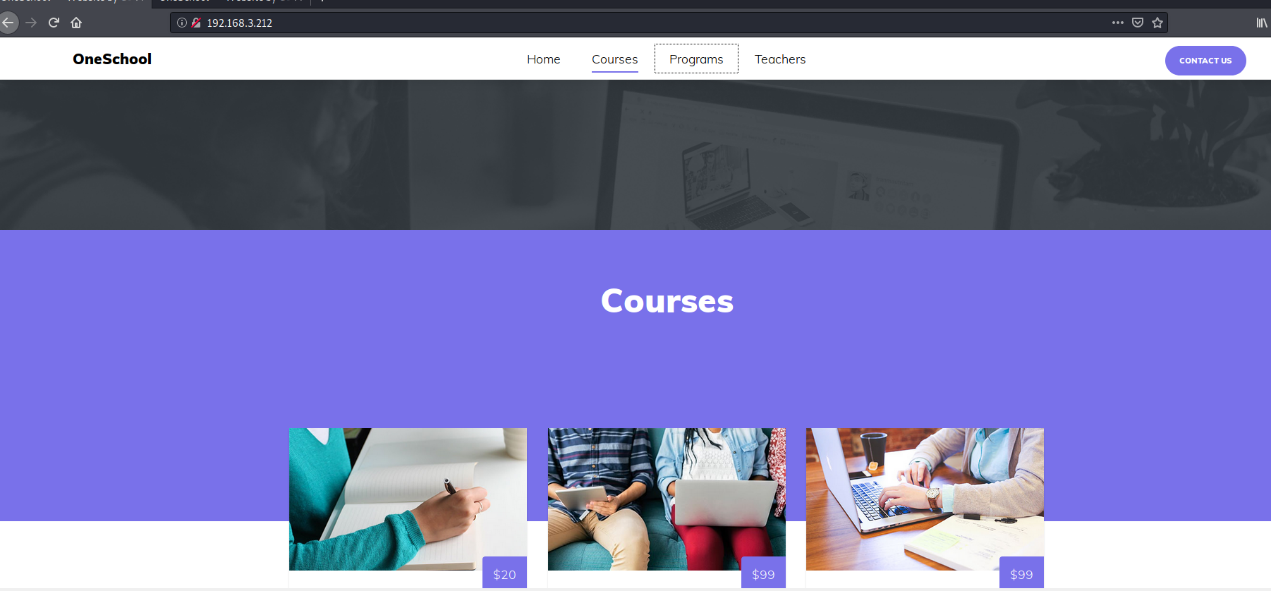


然后开始用nmap探测波端口,这次开了21，22和80虽然21可以Anonymous登录但是里面没有东西所以放弃了

命令:nmap -A -sS -sV -v -p- 192.168.3.212

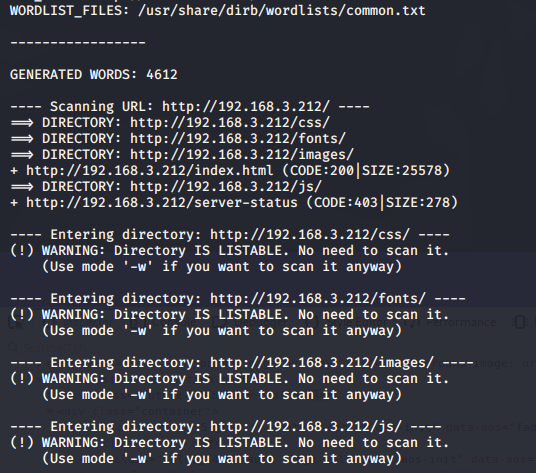


在浏览器输入了波IP可以正常回显有点像一个学校的CMS

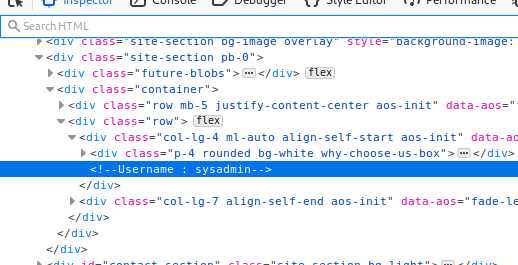


# 0x02:挖掘信息

还是跟往常一样用dirb去80端口探路，但是没有什么有用的信息

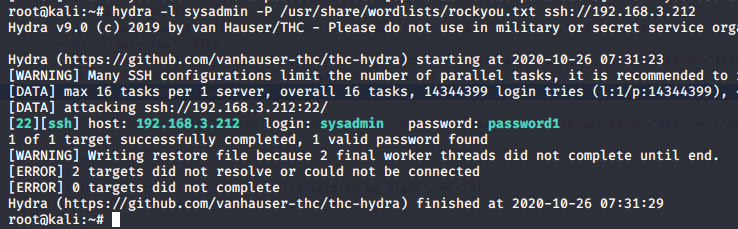


这里只能回到那个首页里面有好几个模块介绍，顺便一边检查网页源代码，一直到Teachers这个模块时有个东西Username:sysadmin,想到介绍的时候提示枚举是关键，可以尝试爆破波22端口

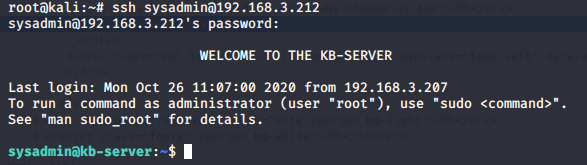


# 0x03:利用Hydra爆破22端口

这里用Hydra跑，没想到是个弱密码很快就跑出来了



直接SSH连接成功

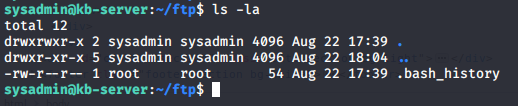


# 0x04:再次挖掘信息

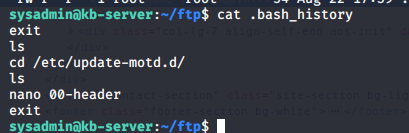
顺便得到user的flag



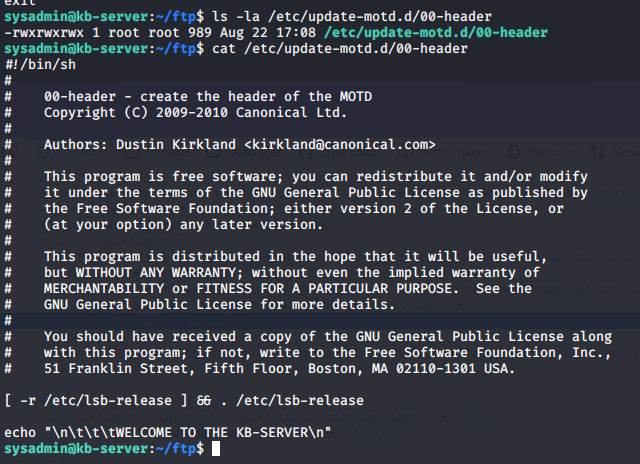
此时来到/home/sysadmin里面顺便发现有个ftp目录跟进以下用ls -la发现个.bash\_history



.bash\_history可以理解为用户曾经在Linux输入过的命令，探查一波发现曾经去到/etc/update-motd.d目录下创建了个00-header(nano跟vim一样也是编辑器，如果 nano+未曾创建过的文件名会在目录下创建一个文件并打开)同时这里查了以下00-header好像是编辑登录22端口以后的欢迎消息



用ls -la看了波权限是root的然后用cat看了下里面的内容



# 0x05:提权

这里有个想法可以在00-header里面用echo添加一个find权限(具备可读可写可运行，方便利用,为什么不用sudo -l?无法利用没得特权。。。。。。。。),添加成功没有报错



关于find提权可以参考回之前做DC-1的提权方法，先创建一个名为test的文件，然后用 find 文件名 -exec 你想要的命令 \;这样，这里输入whoami可以看到已经变成root了。然后看看/root目录下有个flag.txt最后cat一波得到最后的flag。

