尽善尽美的环境确实难找，自己搭建一个

有点不尽人意的是主机模式不管用什么网卡，虚拟机都能互相ping同（导致目前只能搭建一个二层的内网环境），不过万变不离其宗，多级只是多了路由和端口的转发

一.准备工作

4台虚拟机

1.kali攻击机

2.centos7 做网关路由之用

3.windows7靶机，phpstudy开启等web服务

4.ubuntu bwapp靶机

二.vm设置

4台虚拟机相应网络设置

kali虚拟机： 桥接设置 （这样才不能ping通仅主机模式的两台靶机）

centos7：可以添加一块网卡，两块网卡，一块nat模式（vm8网卡），进行外网通信，一块仅主机模式（vm1网卡），进行内网通信

win7靶机： 仅主机模式（vm1网卡）

bwapp靶机： 仅主机模式（vm1网卡）

对centos7模拟路由进行端口转发，以便仅主机模式的两台靶机能通外网：iptables -t nat -A POSTROUTING -s 192.168.74.0/24 -o ens33 -j MASQUERADE  
-s 跟内网网段 -o 跟外网网卡

内网的主机设不设置网关（centos7内网ip地址），自行测试

内网ping www.baidu.com可能ping不通，ping ip行

三.msf+ew进行测试

这个提一点，个人在bind vps主机时，出现meter会话直接关闭，目前不清楚原因

所以目前仅做了端口转发

个人另一篇：http://www.youknowi.xin/2019/04/msfew%e8%bf%9b%e8%a1%8cvps%e7%ab%af%e5%8f%a3%e8%bd%ac%e5%8f%91/

四.msf+cobaltstrike

这个是没有问题

参考：个人另一篇详细过程（安装到测试）

http://www.youknowi.xin/2019/02/%e6%b8%97%e9%80%8f%e6%b5%8b%e8%af%95%e7%a5%9e%e5%99%a8cobalt-strike%e8%bf%9b%e8%a1%8c%e5%86%85%e7%bd%91%e6%b8%97%e9%80%8f/

五.meter会话的几个命令

就这几个常用，其他扫描命令加run直接跑就行了

参考：

https://www.jianshu.com/p/cfa90c8a900f centos 不休眠  
https://www.freebuf.com/column/154125.html  
https://www.secfree.com/a/551.html  
https://blog.csdn.net/m0\_37438418/article/details/79760244  
https://www.cnblogs.com/blck/p/5012355.html msf 内网模块  
https://rcoil.me/2017/10/Jboss%E5%BC%95%E8%B5%B7%E7%9A%84%E5%86%85%E7%BD%91%E6%B8%97%E9%80%8F/

? 获取命令帮助  
具体获取被攻击目标内网地址网段的命令  
run get\_local\_subnets  
run autoroute -s 192.168.42.0/24 添加路由  
backgroup //回到sessions  
getuid 得到uid  
run autoroute -p //查看路由  
run autoroute -d -s 172.2.175.0 //删除网段  
run post/windows/gather/arp\_scanner RHOSTS=192.168.11.0/24 //探测该网段下的存活主机。  
run scanner/mssql/mssql\_ping RHOSTS=192.168.11.0/24 threads=30  
ps //查看pid等  
migrate //进程迁移，很有用，找到system pid，迁移，才能hashdum

2019.4.10