实战ATT&CK攻击链路--靶场Writeup(二)

原创

Ms08067安全实验室 于 2021-11-01 08:00:00 发布 85 收藏
文章标签： 安全 人工智能 java 编程语言 信息安全

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

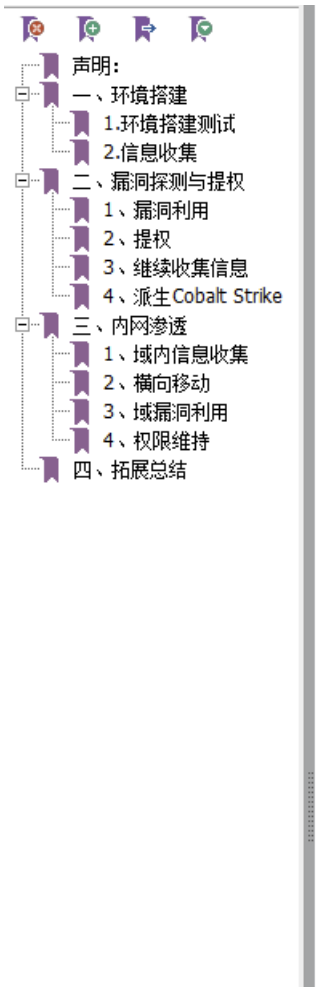
成立"安全练兵场"的目的

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/3/

本次主要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。关于靶场统一登录密码：1qaz@WSX



公众号后台回复：“MS08067安全练兵场星球2”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。

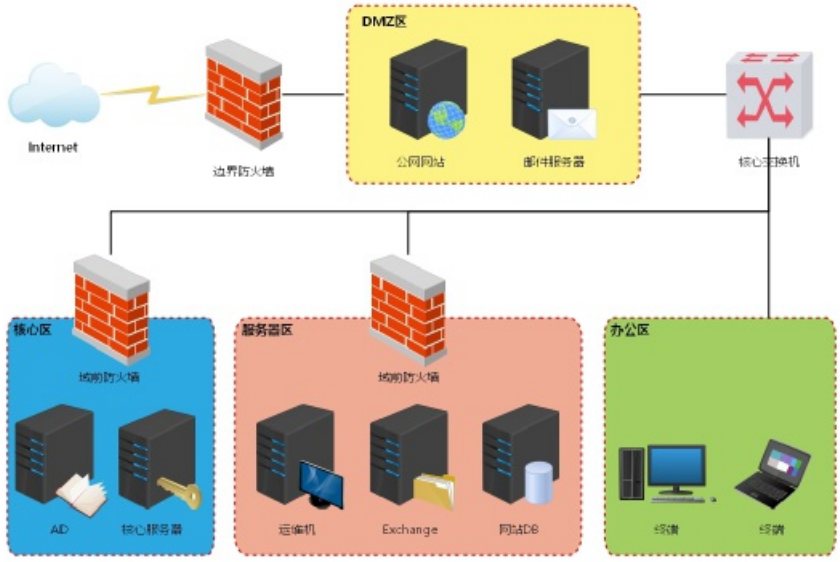
第二阶段：Portswigger是著名神器Burpsuite的官方网站，是一个很好的漏洞训练平台，Burpsuite学院目前含有漏洞实验内容160多个，基本涵盖了各个方面的Web漏洞，并且会不断更新。

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！

号外：

11.5号 红队攻防 第4期 再次来袭

课程费用

每期班定价**2999**，**第四期班早鸟价：2499**（支持信用卡、花呗分期，可开发票），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！

付一期班钱，听2期班课！
你还在犹豫什么？

学习资源

前40名报名同学，送499元内网知识星球名额，可提前先行学习内网渗透相关知识，并提供课程中需要的相关软件和环境。

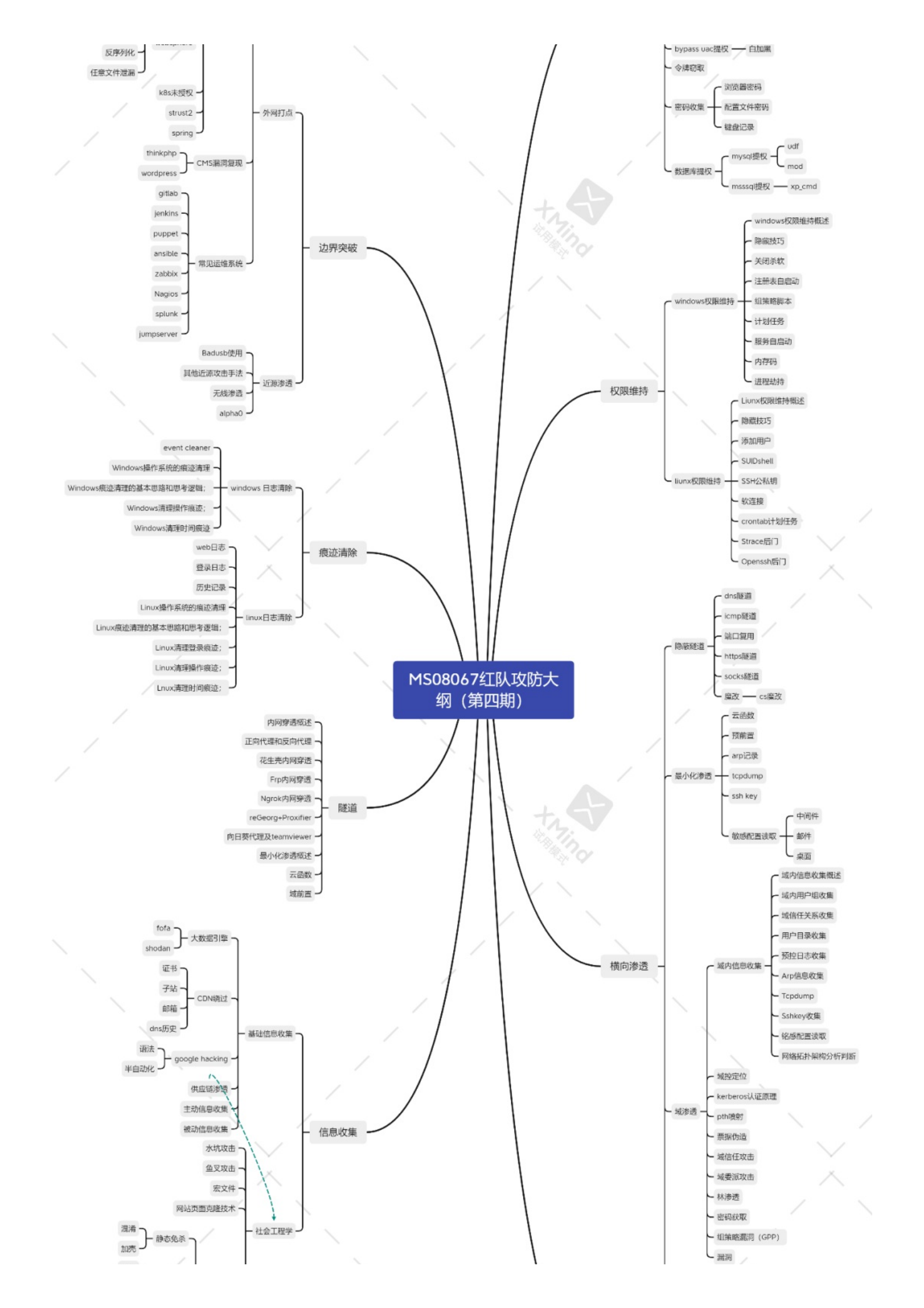
上课时间

每周五、六、日的晚间 19：30-21:30 ，共23课时，为期二个月。
如果无法准时参加直播课程，在线培训的每节课程都会被录制成视频（一机一码）上传到学员区，可随时下载观看。

上课方式

培训采用在线直播+随堂录播+微信群解答 的形式，无需等待，报名后立即进入“内网星球”开始预习。

全新课程大纲4.0版


MS08067红队攻防大纲（第四期）
边界突破
外网打点
反序列化
任意文件泄漏
k8s未授权
strust2
spring
CMS漏洞复现
thinkphp
wordpress
常见运维系统
gitlab
jenkins
puppet
ansible
zabbix
Nagios
splunk
jumpserver
近源渗透
Badusb使用
其他近源攻击手法
无线渗透
alpha0
痕迹清除
windows 日志清除
event cleaner
Windows操作系统的痕迹清理
Windows痕迹清理的基本思路和思考逻辑；
Windows清理操作痕迹；
Windows清理时间痕迹
linux日志清除
web日志
登录日志
历史记录
Linux操作系统的痕迹清理
Linux痕迹清理的基本思路和思考逻辑；
Linux清理登录痕迹；
Linux清理操作痕迹；
Lnux清理时间痕迹；
隧道
内网穿透概述
正向代理和反向代理
花生壳内网穿透
Frp内网穿透
Ngrok内网穿透
reGeorg+Proxifier
向日葵代理及teamviewer
最小化渗透概述
云函数
域前置
信息收集
基础信息收集
大数据引擎
fofa
shodan
CDN绕过
证书
子站
邮箱
dns历史
google hacking
语法
半自动化
供应链渗透
主动信息收集
被动信息收集
社会工程学
水坑攻击
鱼叉攻击
宏文件
网站页面克隆技术
静态免杀
混淆
加壳
权限维持
bypass uac提权
白加黑
令牌窃取
密码收集
浏览器密码
配置文件密码
键盘记录
数据库提权
mysql提权
udf
mod
mssql提权
xp_cmd
windows权限维持
windows权限维持概述
隐藏技巧
关闭杀软
注册表自启动
组策略脚本
计划任务
服务自启动
内存码
进程劫持
liunx权限维持
Liunx权限维持概述
隐藏技巧
添加用户
SUIDshell
SSH公私钥
软连接
crontab计划任务
Strace后门
Openssh后门
横向渗透
隐蔽隧道
dns隧道
icmp隧道
端口复用
https隧道
socks隧道
魔改
cs魔改
最小化渗透
云函数
预前置
arp记录
tcpdump
ssh key
敏感配置读取
中间件
邮件
桌面
域渗透
域内信息收集
域内信息收集概述
域内用户组收集
域信任关系收集
用户目录收集
预控日志收集
Arp信息收集
Tcpdump
Sshkey收集
铭感配置读取
网络拓扑架构分析判断
域控定位
kerberos认证原理
pth喷射
票据伪造
域信任攻击
域委派攻击
林渗透
密码获取
组策略漏洞（GPP）
漏洞

你距离红队大佬，只差一个决定

详情咨询请联系小客服

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！

Java代码安全审计【Ms08067】

星主： 徐哥

知识星球

微信扫描预览星球详情

Ms08067安全实验室

内网攻防【Ms08067】

星主： 徐哥

知识星球

微信扫描预览星球详情

Ms08067安全实验室

目前50000+人已关注加入我们