

实战ATT&CK攻击链路--靶场Writeup(一)

原创

Ms08067安全实验室 于 2021-10-25 08:00:00 发布 251 收藏 2

文章标签: [安全](#) [人工智能](#) [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/120963824

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)

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/2/>

红队实战系列, 主要以真实企业环境为实例搭建一系列靶场, 通过练习、视频教程、博客三位一体学习。

另外本次实战完全模拟ATT&CK攻击链路进行搭建, 开成完整闭环。后续也会搭建真实APT实战环境, 从实战中成长。关于环境可以模拟出各种各样实战路线, 目前给出作者实战的一套攻击实战路线如下, 虚拟机所有统一密码: hongrise@2019

- 声明:
- 一、环境搭建
 - 1.环境搭建测试
- 二、漏洞利用
 - 3.漏洞搜索与利用
 - 3.1 弱口令漏洞登录后台
 - 3.2 phpmyadmin弱口令漏洞
 - 3.3 目录遍历漏洞
 - 3.5 XSS
 - 4.后台Getshell上传技巧
 - 5.系统信息收集
 - 6.主机密码收集
 - 6.1 反弹shell连接 (php载荷)
 - 6.2 反弹shell连接 (windows载荷)
 - 6.3 提权
 - 6.4 获取密码
- 三、内网搜集
 - 7.内网-继续信息收集
 - 7.1 补丁信息
 - 7.2 软件安装信息
 - 7.3 路由信息并添加路由
 - 7.4 arp扫描内网主机
 - 7.5 内网扫描
 - 8.内网攻击姿势-信息泄露
 - 9.内网攻击姿势-MS08-067 (失败)
 - 10.内网攻击姿势-SMB远程桌面口令猜测 (成功)
 - 11.内网攻击姿势-Oracle数据库TNS服务漏洞 (失败)
 - 12.内网攻击姿势-RPC DCOM服务漏洞 (失败)
 - 附1: 内网攻击姿势-MS17-010 (成功)
 - 附2: 内网攻击姿势-MS17-010
- 四、横向移动
 - 13.内网其它主机端口-文件读取
 - 14.内网其它主机端口-redis
 - 15.内网其它主机端口-redis Getshell
 - 16.内网其它主机端口-Mysql数据库
 - 17.内网其它主机端口-Mysql提权
- 五、构建通道
 - 18.内网其它主机端口-代理转发
 - 18.1 将tunnel.php上传到win7
 - 18.2 配置 proxychains 使用 socks5 代理
 - 18.3 启动 neoreg.py 时指定的 IP 地址和端口
 - 18.4 代理扫描
- 六、持久控制
 - 附3: 混生 Cobalt Strike
 - 1. Cobalt Strike 上线主机
 - 2. Cobalt Strike 金票利用
 - 19.域渗透-域成员信息收集
 - 20.域渗透-基础服务弱口令探测及深度利用之powershell
 - 21.域渗透-横向移动(wrm利用)
 - 22.域渗透-C2命令执行
 - 23.域渗透-利用DomainFronting实现对beacon的深度隐藏
 - 24.域渗透-域控实现与利用
 - 附4: 后门植入
 - 1.persistence 启动项后门
 - 2.metsvc 服务后门
- 七、痕迹清理
 - 25、日志清理
 - 1.手动清理
 - 2.使用工具清除 windows 日志
 - 3.使用脚本工具停止系统日志记录
- 相关链接

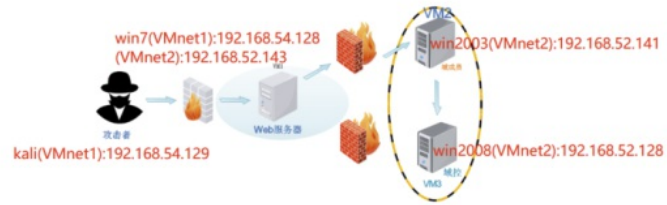
声明:

本文仅供学习网络安全行业的朋友们参考，同时是记录自己成长的随笔记录，其中涉及的一切资源均来自于网络，请勿用于任何非法行为，否则您将自行承担相应后果，我们将不承担任何法律及连带责任。

一、环境搭建

1.环境搭建测试

1.1 网络所示



2.信息收集

2.1 端口扫描

nmap扫描web主机端口，发现开放了80、3306，大部分端口被过滤，判断存在防火墙。

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-10 15:17 CST
Nmap scan report for 192.168.54.1
Host is up (0.00012s latency).
MAC Address: 00:50:56:C0:00:01 (VMware)
Nmap scan report for 192.168.54.128
Host is up (0.00019s latency).
MAC Address: 00:0C:29:86:1B:F7 (VMware)
Nmap scan report for 192.168.54.254
Host is up (0.000099s latency).
MAC Address: 00:50:56:FB:10:4B (VMware)
Nmap scan report for 192.168.54.129
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 27.97 seconds
root@kali:~# nmap 192.168.54.128
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-10 15:18 CST
Nmap scan report for 192.168.54.128
Host is up (0.00036s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 00:0C:29:86:1B:F7 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 24.91 seconds
```

2.2 WEB站点探测

公众号后台回复：“MS08067安全练兵场星球1”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...

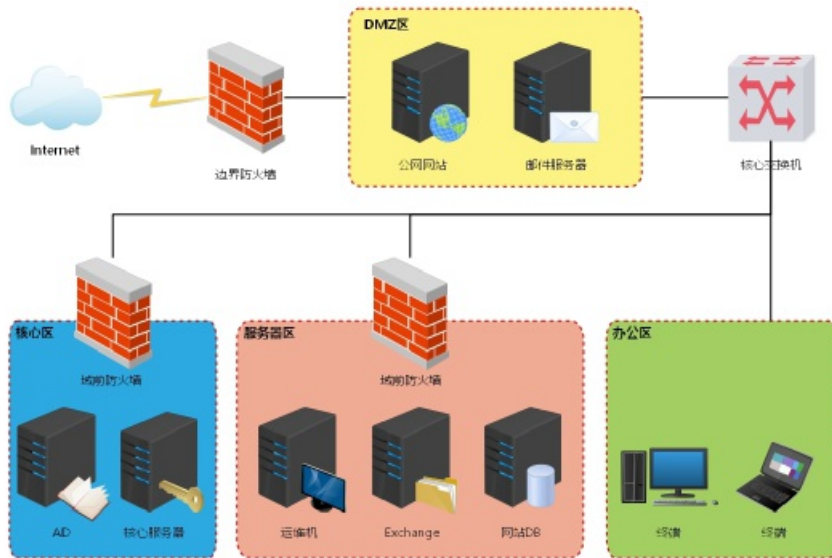
讲师：

Godunt，某国内知名内网威胁管理公司高级工程师，极度热衷于Web安全、内网渗透及安全攻防技术。

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！

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

