MS08067 “安全练兵场”战术空袭~

原创

Ms08067安全实验室 于 2021-10-18 22:36:10 发布 1728 收藏 13
文章标签： 人工智能 安全 编程语言 信息安全 java

本文链接：https://blog.csdn.net/shuteer_xu/article/details/120837963

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。

"安全练兵场"星球de后续方向

1.国内外优质靶场推荐及Writeup分享（模拟真实的攻防环境）

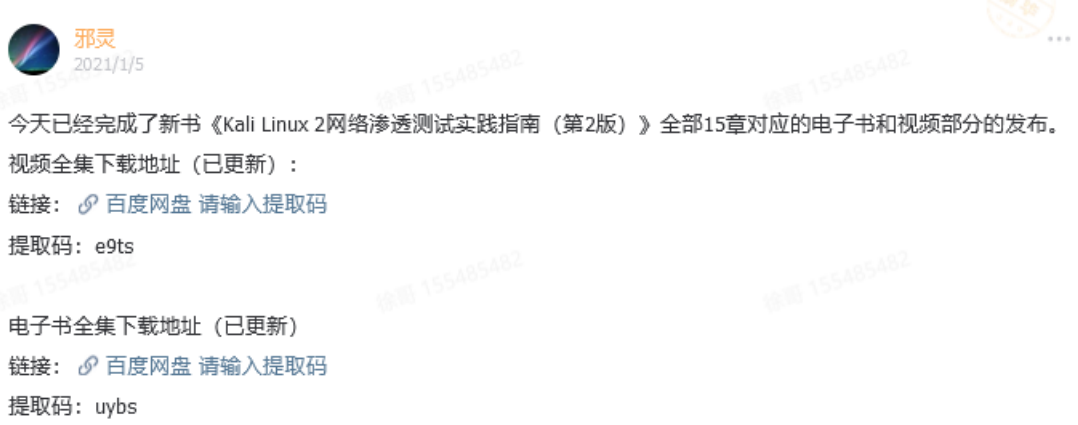
2.实战安全攻防工具讲解及拓展

3.实战分享（护网资源、威胁情报、勒索挖矿、应急响应、漏洞复现等）

4.最新的技术文章的原创翻译和视频讲解

"安全练兵场"星球 由 “Kali安全”星球 升级而成

截止目前，“Kali星球”已经完成了《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，并且在星球内部配备了电子书，以便学习！



实验所涉及的所有【配套教案PPT、虚拟机环境及靶机环境】也已经调试好，下载即可使用。

邪灵
2021/3/2

星球重点资源汇总部分，方便大家查找内容，将之前主要内容汇总到这一个帖子中来。

1、《Kali Linux 2渗透测试指南先导课程》（这部分主要是Kali linux中的文件和命令部分，没在实体书中出现，没有linux操作基础的同学可以先学习一下）
视频部分：
链接：百度网盘 请输入提取码
提取码：k3u4

电子书部分：
链接：百度网盘 请输入提取码
提取码：pk9h

2、《Kali Linux 2网络渗透测试实践指南（第2版）》实体书对应的电子版和视频部分的发布。
视频全集下载地址）：
链接：百度网盘 请输入提取码
提取码：e9ts

电子书全集下载地址
链接：百度网盘 请输入提取码
提取码：uybs

PPT（视频录制后重新制作新版，所以有所不同）下载链接为：
链接：百度网盘 请输入提取码
提取码：dvup

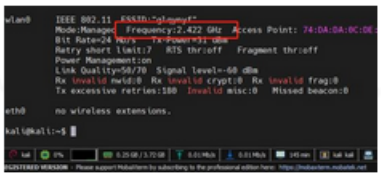
3、Kali Linux 2网络渗透测试实践指南（第2版）》中使用的资源，

Kali linux 2020.1（Vmware版本，本书所使用的kali版本）
链接：百度网盘 请输入提取码
提取码：h3i0
windowsxp靶机
链接：百度网盘 请输入提取码
提取码：c886
windows7$64位靶机
链接：百度网盘 请输入提取码
提取码：4ih1
windows7$32位靶机
链接：百度网盘 请输入提取码
提取码：3a56
linux靶机
链接：百度网盘 请输入提取码
提取码：c67n

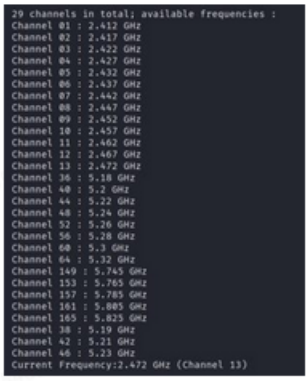
在学习过程中针对所学技术点产生任何疑问可以随时在星球提问，也可以通过我们的永久微信群相互交流！

邪灵
2021/2/23

> Abathur 提问： 我有两个树莓派一个3b一个4b，两个都安装了kali，但是有一个问题3b可以使用5g的wifi，4b的只能使用2.4g的wifi 。两点树莓派的内存卡互换过问题一样。使用的的kali版本是2020.4。
> 请问大佬有注意过这个问题吗



树莓派连接之后的Frequency是由连接的wifi决定的，但是也需要树莓派的无线网卡的支持，你可以首先用iwlist channel命令查看一下当前设备支持的channel，例如我的设备当前支持的如图所示，超出这些channel的设备就不支持了，你可以试试将wifi的channel设置成其中支持的数值。



查看详情

windy 觉得很赞

> Abathur ： 设备本身没问题的，外置的网卡也是一样，我使用的AP是双频的。
>
> 3b4b的内存卡我互换过，就4b的有问题 查看图片
> 2021/2/23
>
> 邪灵 回复 Abathur ： 那你试试修改树莓派上WiFi的地区。使用rasp-config或图形界面里的设置将地区改为US，同时需要路由器上把地区也修改为US
> 2021/2/23
>
> Abathur 回复 邪灵：里面安装的是kali，我AP的信道是149，iwlist channel里面也有，关键就是4b有这个问题，3b就是好的
> 2021/2/23
>
> 邪灵 回复 Abathur ： 这个跟操作系统没关系，树莓派3b和4b都有这个问题，可能你的3b里国家已经设置为US了。
> 2021/2/23
>
> Abathur 回复 邪灵：内存卡是同一个，什么都没变就是3b4b变了
> 2021/2/23
>
> 邪灵 回复 Abathur ： 我现在手头没有3b+这个型号的树莓派，所以没法测试。硬件上3b+和4b都是支持5G的，像你这种情况，具体原因我也不清楚，不过如你想4B上网，可以试试我上面说的方法。
> 2021/2/23
>
> Abathur 回复 邪灵：你的图链接的也是2.4的无线，是4b的板子吗，还是只有2.4的ap
> 2021/2/23
>
> 邪灵 回复 Abathur ： 我家里的ap没有5g功能，图是在虚拟机里截的
> 2021/2/23

下一阶段目标

“Kali安全”星球升级为“安全练兵场”星球后

第一个阶段：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...

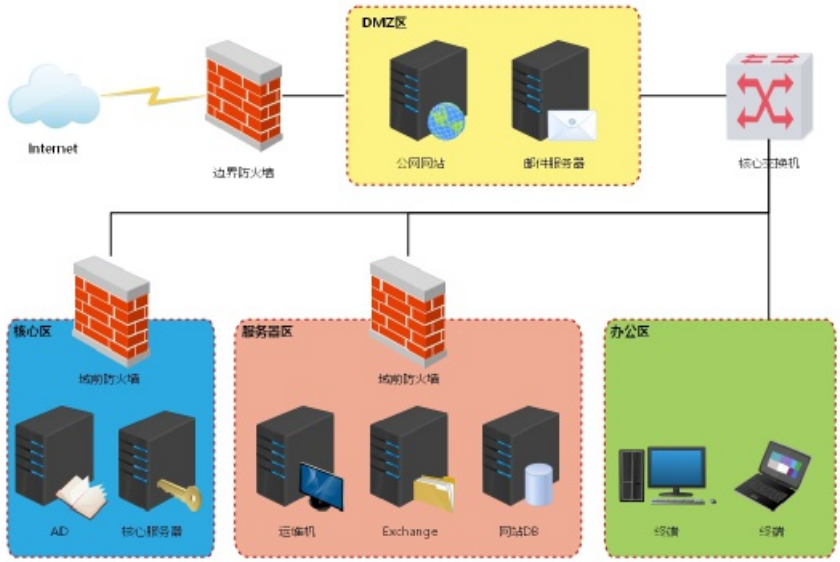
讲师：

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。

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。

奖励计划

我们征集优秀的靶场Writeup及靶场推荐，奖励多多！

最后

感谢红日团队提供的安全靶场

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

WEB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

0基础逆向【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

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