[网络安全自学篇] 一.入门笔记之看雪Web安全学习及异或解密示例

转载

cookie-niu 于 2019-08-27 22:33:25 发布 413 收藏 4
分类专栏： 服务器
原文链接：https://blog.csdn.net/Eastmount/article/details/97784774

本文链接：https://blog.csdn.net/Eastmount/article/details/97784774

最近开始学习网络安全相关知识，接触了好多新术语，感觉自己要学习的东西太多，真是学无止境，也发现了好几个默默无闻写着博客、做着开源的大神。准备好好学习下新知识，并分享些博客与博友们一起进步，加油。非常基础的文章，大神请飘过，谢谢各位看官！

前文欣赏：
[渗透&攻防] 一.从数据库原理学习网络攻防及防止SQL注入
[渗透&攻防] 二.SQL MAP工具从零解读数据库及基础用法
[渗透&攻防] 三.数据库之差异备份及Caidao利器
[渗透&攻防] 四.详解MySQL数据库攻防及Fiddler神器分析数据包

文章目录

一.工具&术语

1.网安术语

常见安全网站及论坛：

看雪（https://bbs.pediy.com/）
安全客（https://www.anquanke.com）
freebuf（https://www.freebuf.com/）
安全牛（https://www.aqniu.com/）
安全内参（https://www.secrss.com/）
绿盟（http://www.nsfocus.com.cn/）
先知社区（https://xz.aliyun.com/）

++

基础知识：

风险评估
1）渗透测试技术：踩点扫描探测、信息收集、暴力破解、漏洞扫描、Web权限获取、Web提权、溢出攻击、植入后门、内网渗透等。
2）安全漏洞的代码审计和代码加固技术：缓冲区溢出、拒绝服务、远程命令执行、注入、跨站、Web提权。

安全防护
1）中间件和Web应用的安全监测与防护方法：框架漏洞、权限绕过、弱口令、注入、跨站、文件包含、文件上传、命令执行、任意文件读取和下载等。
2）主流厂商网络安全设备的调试与配置；主流数据库系统的补丁、账号管理、口李玲强度、有效期检查、远程服务、存储过程、审核层次、备份过程、用户功能和权限控制等基础技术；数据库库内库外加密、硬件加密、数据库审计技术；操作系统安全管理、客户端访问控制、入侵检测技术、数据异地灾备等技术。
3）主机操作系统和应用软件的安全配置、主机运行的应用程序、正常运行所需端口，服务的正确配置，涉及系统安全风险测试、文件系统、关键数据、配置信息、口令用户权限等内容。

应急响应
1）应急响应相关技术：入侵取证分析、日志审计分析等。
2）操作系统常规安全防护技术：利用系统日志、应用程序日志等溯源共计途径，系统账号、文件系统、网络参数、服务、日志审计等项目安全监测与安全加固方法。
3）网络设备和安全设备的功能及使用方法：路由器、交换机、防火墙、入侵检测系统、拒绝服务供给系统、网页防篡改系统、漏洞扫描系统等。

安全加固
1）操作系统（Windows、Linux、Unix、Mac）的常规安全防护技术：利用系统日志、应用程序日志等溯源攻击途径，统账号、文件系统、网络参数、服务、日志审计等项目安全监测与安全加固方法。
2）Webcms、中间件、数据库等常规用Web应用的加固知识，应用防火墙、IPS、IDS等安全设备进行辅助加固措施。

大数据安全
1）云计算和大数据技术带来的安全问题：虚拟机安全、应用程序安全、大数据安全。
2）大数据分析技术提升网络系统安全隐患发现和防护能力。

物联网安全
1）ID/IC卡的安全漏洞检测和发现技术，智能卡常见加密算法。
2）物联网应用环境中典型安全攻击：RFID攻击等。
3）无线安全、硬件安全等知识。

其他
1）密码学概念、加密算法、加密分析工具。
2）网络攻击原理及常见网络攻击协议，数据包分析工具。
3）Web攻击种类及常见的Web利用方式，注入攻击类型及方式。
4）漏洞产生原因、漏洞的利用与防护方式。
5）恶意代码、逆向工程、沙箱保护。
6）移动互联网恶意程序检测与处置机制，移动逆向分析与代码审计技术、移动安全防护。
7）数据恢复常用技术及工具。
8）工业控制系统、工控漏洞及加固分析、工控漏洞玩、工控安全仿真及蜜罐、工控系统上位机及应用安全等。

++

常见攻击手段：

扫描
破解
溢出
木马病毒
Web攻击
无线攻击
VPN劫持
Kali攻击
MAC泛洪攻击
时钟攻击

++

常见术语：

0day
动态分析、静态分析
逆向分析
PE文件
注册回调
HOOK技术
注入技术
加壳、脱壳、加花
社会工程学
供应链渗透
SAM哈希暴力
彩虹表
数据取证
可信计算

++

————————————————