

i春秋与我

转载

[weixin_30306905](#) 于 2017-03-04 23:42:00 发布 73 收藏
原文链接: <http://www.cnblogs.com/arsense/p/6503295.html>
版权

春秋
培育信息时代的安全感

搜索课程、竞赛或讲师

下载App D_Clay

首页 知识体系 职业成长 竞赛训练 企安殿 SRC部落 NEW 社区

名企安全 >
企业安全 >
网站安全 >
客户端安全 >
通信安全 >
移动安全 >
智能硬件安全 >
工控安全 >
安全理论 >
CTF学习 >

本周课表

周一	周二	周三	周四	周五

- DDoS三连击: 半个美国互联网的瘫痪
- Node.js 反序列化漏洞远程执行代码...
- PWN简介与学习方法

本周快讯

- [360SRC] 季度奖励: 带你最爱的...
- [蚂蚁金服SRC] 你青涩的第一次, ...
- [宜人贷SRC] 吐槽大会开始了-
- [唯品会SRC] 我的ELK搭建笔记...

快速链接

闪电实验室 先到先得瞬间开启

App下载 SRC部落 公开课

Word文档安全防护

CVE-2016-5195 (脏牛) 内核提权...

无处不在的SQL注入

在i春秋论坛混迹了大半年了,在i春秋的在线平台学到了很多奇技淫巧,特别喜欢这个平台的气氛,以及虚拟在线网络环境的搭建,

忙周偷乐,过来也为i春秋做点小奉献,共同构造我们喜欢的春秋平台,成长特别快,特别时尚优秀的一个平台,看着CTF工具库从几行文字的网页

变成现在动态丰富的平台,甚是欣慰,让我也出一点微博之力。所以整个一天都在和负责人交流,如何配置流程,实验环境。开始我的i春秋新旅程

我这正在火热进行中,希望得到大家的支持

CTFTools

致力于为CTFer提供便利

[关于](#)[资源库](#)[HBCTF](#)[加群得TOKEN](#)

下面是我即将实验配置录制的课程，希望能丰富大家的网络安全知识，不要随便连公共wifi哦

- IPC\$共享空连接实验。
 - Windows 系统弱口令 [ipc](#) 命令攻击技术。
- Windows 口令安全加固。
 - 通过开启组策略编辑设置账户锁定 ,审核,权限, 修改默认账号等。
- Windows 系统口令提取与破解。
 - 使用 [GetHashes](#)、[Ophcrack](#)、[saminside.WinlogonHack](#) 等一系列工具。
- Windows 系统明文抓取。
 - 通过使用 [mimikatz](#) 等工具抓取。
- 系统密码破解工具。
 - [GetHashes](#)、[Ophcrack](#)、[saminside.WinlogonHack](#) 等一系列工具。

- Sniffer 劫持实验
 - Kali-Linux 中的 ettercap 进行劫持
- ARP 劫持实验
 - 使用 Kali-Linux 中的 ettercap 进行劫持 欺骗
- Hook 劫持实验
 - 使用 Kali-Linux msfconsole 控制台实现 Hook 攻击
- 钓鱼实验
 - 先使用 ettercap 进行 Arp 劫持然后 ferret 抓取数据包, 使用 hamster 架设代理, 登陆会话

明文密码拦截.MD
X

```
#### 步骤1: 启动ettercap, 配置目标信息
#### 步骤2: 进行arp欺骗
#### 步骤3: 抓取本地数据包
#### 步骤4: 使用ferret分析抓取的数据包
#### 步骤5: 监听获取hamster架设代理, 登录会话, 获得密码
### Part 3 Hook劫持

#### 步骤1: 在msfconsole使用search命令搜索MS08067漏洞攻击程序
#### 步骤1: 使用use命令调用MS08067漏洞攻击程序
#### 步骤1: set 命令设置 Module Options
#### 步骤1: 设置Exploit target
### Part 4 钓鱼
#### 步骤1: 建立热点
工具: isc-dhcp-server ; Aircrack-ng套件; iptables

建立过程:

首先写dhcp配置文件/etc/dhcp/dhcpd.conf
#### 步骤2: 劫持DNS
dnscchef -i 10.0.0.1 --nameserver 210.73.64.1#53
#### 步骤3: 把淘宝和百度(钓鱼网站)解析到本机
```

明文密码拦截

实验目的

- 熟悉使用Kali-Linux的基础工具使用
- 掌握Sniffer劫持, ARP劫持, HOOK劫持, 钓鱼的原理与使用

实验环境

- 操作机: Kali-Linux
 - Ettercap最初设计为交换网上的sniffer, 但是随着发展能, 成为一款有效的、灵活的中介攻击工具。它支持了许多网络和主机特性(如OS指纹等)分析。
 - msfconsole是目前Metasploit框架最为流行的用户接口为MSF终端是Metasploit框架中最灵活、功能最丰富及MSFCONSOLE主要用于管理Metasploit数据库, 管理模块。本质上来说, 就是为了利用漏洞, MSFCONSOLE信息, 以至于用户能启动渗透攻击目标系统。本小节将(MSFCONSOLE)。

转载于: <https://www.cnblogs.com/arsense/p/6503295.html>