CTF资源

原创

烟火里的尘埃呐 于 2021-08-05 08:39:02 发布 364 收藏 1

分类专栏： 资源 文章标签： unctf

本文链接：https://blog.csdn.net/weixin_53579562/article/details/119294069

资源 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

一 个人成长

```
此部分内容来自 TK 教主分享的腾讯玄武实验室内部例会 PPT 资料。
```

1 个人成长

```
确立个人方向，结合工作内容，找出对应短板：

该领域主要专家们的工作是否都了解？
相关网络协议、文件格式是否熟悉？
相关的技术和主要工具是否看过、用过？

阅读只是学习过程的起点，不能止于阅读：

工具的每个参数每个菜单都要看、要试。
学习网络协议要实际抓包分析，学习文件格式要读代码实现。
学习老漏洞一定要调试，搞懂别人代码每一个字节的意义，之后要完全自己重写一个 Exploit。
细节、细节、细节，刨根问底。
```

2 建立学习参考目标

```
短期参考什么？比自己优秀的同龄人：

阅读他们的文章和其它工作成果，从细节中观察他们的学习方式和工作方式。

中期参考什么？你的方向上的业内专家：

了解他们的成长轨迹，跟踪他们关注的内容。

长期参考什么？业内老牌企业和先锋企业：

把握行业发展、技术趋势，为未来做积累。
```

3 推荐的学习方式

```
以工具为线索：

一个比较省事的学习目录：Kali Linux。
学习思路，以 Metasploit 为例：遍历每个子目录，除了 Exploit 里面还有什么？/ 每个工具分别有什么功能？原理是什么？涉及哪些知识？/ 能否改进优化？能否发展、组合出新的功能？

以专家为线索：

你的技术方向里有哪些专家？
他们的邮箱、主页、社交网络帐号是什么？
他们在该方向上有哪些作品？发表过哪些演讲？
跟踪关注，一个一个学。
```

4 处理好学习、工作、生活

```
学习、工作和生活是矛盾统一的。

三者都需要时间，你一天只有 24 小时：调和矛盾的关键是提高效率。

对没有一个好爸爸的人来说，你的学习、工作会影响你能不能追求诗和远方。

有好爸爸也要学习，因为能力之外的资本等于零。
```

5 如何提高效率

```
做好预研，收集相关前人成果，避免无谓的重复劳动。

在可行性判断阶段，能找到工具就不写代码，能用脚本语言写就不要用编译语言，把完美主义放在最终实现阶段。

做好笔记并定期整理，遗忘会让所有的投入都白白浪费。

多和同事交流，别人说一个工具的名字可能让你节约数小时。

咖啡可以提高思维效率，而且合法。

无论怎么提高效率，要成为专家，都需要大量的时间投入。
```

二 信息安全职业方向、职业规划

```
信息安全职业方向：
信息安全职业方向

信息安全职业规划：
信息安全职业规划

补充，Hacker 学习发展流程图：
Hacker 学习发展流程图
```

三 知识体系构建

理论 + 学习目录 + 实践。

```
理论：理论相关课程（数学，计算机基础知识，信息安全专业相关课程等）。
学习目录：Kali Linux。
实践：CTF。
```

1 理论相关课程、学习路线、书籍

整体知识域概况（博主自己整理的）：
整体知识域概况

数学课程：

《高等数学》
《线性代数》
《概率论与数理统计》
《离散数学》
《具体数学》

计算机基础知识课程：

《计算机组成原理》
《操作系统》
《数据结构与算法》
《计算机网络》
《数据库系统原理》
《软件工程》

信息安全相关课程、学习路线：

（重要参考文档）网络空间安全工程技术人才培养体系指南
安全电子书籍红日攻防推荐：链接
信息安全从业者书单推荐：来自 riusksk 的 GitHub 分享
信息安全行业认证 CISSP 学习资料推荐：Cybrary 的 CISSP 教学视频，Google/youtube 相关视频，官方的 CISSP APP（study+exam），CISSP 11小时，官方教材。
技能时间轴：链接
安全技能树简版 by 余弦：链接
知道创宇研发技能表：链接
漏洞银行 (BUGBANK) 技能树：链接
信息安全思维导图集合：来自 SecWiki 的 GitHub 分享
安全类思维导图 by phith0n：链接

2 信息安全专业课程体系

来自实验吧：链接

计算机基础课：

《计算机基础》是学生对计算机有初步认知的课程。
《C/java语言程序设计》是学生对编程的初步认知，有助于后续理解计算机原理及程序漏洞成因。
《信息安全数学基础》会重要介绍与信息安全相关的数据基础，有助于对于后续理解密码学算法及应用。
《信息安全导论》会初步介绍信息安全的体系架构，是学生对信息安全的技术和管理体系有初步认知。

信息安全专业基础课：

《网络协议分析》
《TCP/IP路由与交换技术》
《微机原理与汇编语言》
《数据库原理与应用》
《Python编程技术》
《操作系统原理》
《Linux系统与服务器管理》
《php+mysql web程序开发》
《信息安全法律法规》

信息安全核心专业课：

《计算机网络安全》
《web安全》
《渗透测试》
《kali渗透》
《安全网关防护设备原理与配置》
《内网入侵检测系统原理与配置》
《恶意代码原理与分析》
《密码学技术与应用》
《智能硬件安全》
《逆向工程》

信息安全专业实训课程：

《网络工程项目实训》
《安全系统集成项目实训》
《渗透测试与应急响应项目实训》
《风险评估项目实训》

3 信息安全专业课程补充

```
课程：链接

系统安全/软件安全系列：

计算机安全与维护
系统与程序设计实践
逆向工程
软件与系统安全

数字内容安全系列：

数字内容安全基础
数字媒体安全应用与实践
计算机安全与维护

网络安全系列：

网络安全
移动互联网安全
Linux 系统与网络管理
信息安全工程实践

密码学应用于实践
```

4 学习目录 Kali Linux

```
Kali Linux 工具分类简介：

Information Gathering（信息收集）
Vulnerability Analysis（漏洞分析）
Web Applications Analysis（Web 程序分析）
Database Assessment（数据库评估）
Password Attacks（密码攻击）
Wireless Attacks（无线攻击）
Reverse Engineering（逆向工程）
Exploitation Tools（漏洞利用工具集）
Sniffing & Spoofing（嗅探/欺骗）
Post Exploitation（权限维持）
Forensics Tools（数字取证）
Reporting Tools（报告工具集）
Social Engineering Tools（社会工程学工具）
System Services（系统服务）

关于 Kali Linux 的学习资料：

Kali Linux 官方文档，链接
kali linux 工具相关：工具使用说明书链接，补充：Kali 工具页面链接，kali 工具列表中文解释
《Kali Linux大揭秘：深入掌握渗透测试平台》，豆瓣读书链接
Kali 渗透测试（大学霸），链接
Kali Linux web 渗透测试经典视频，链接
```

5 CTF 内容、资料、工具、演练平台

```
CTF 入门与分类：

入门：Wiki，链接；CTF 入门视频课程，链接。
分类：国际 CTF 竞赛、国家 CTF 竞赛、企业 CTF、高校CTF。

CTF 内容：
```

CTFs 内容：Web 网络攻防、Reverse Engineering 逆向工程、Pwn 二进制漏洞利用、Crypto 密码攻击、Mobile 移动安全、Misc 安全杂项。
全国大学生信息安全竞赛内容：系统安全、软件逆向、漏洞挖掘和利用、密码学原理及应用、其他内容。

CTF 学习指南：

AB 学习方向：
A 方向：Pwn + Reverse + Crypto。/ B 方向：Web + Misc

需要学的内容：
需要学的内容

A 方向推荐书籍：
A 方向推荐书籍

B 方向推荐书籍：
B 方向推荐书籍

基础题目练习：
idf 实验室，xctf 题库网站，i 春秋 CTF 训练，challs 非常入门的国外 ctf 题库，非常入门的国外 ctf 题库。

A 方向题目练习：
很炫酷游戏化，比较简洁的内容（ssh连入即可玩），
比较老牌的 Wargame（overthewire） 比较老牌的 Wargame（exploit-exercise），PWN 类题目的游乐场。

B 方向题目练习：
米安的 Web 漏洞靶场，国外的 XSS 测试，国外的 sql 注入的挑战网站。

CTF 赛事、竞赛比赛：

CTFtime（All about CTF），链接
XCTF，链接
CTF Rank，链接
全国大学生信息安全竞赛，链接
i 春秋赛事服务，链接

CTF 工具：

CTF 在线工具，链接
CTF 工具资源库，链接

训练演练、竞赛比赛：

Practice CTF List / Permanant CTF List，链接
i 春秋 CTF 训练：链接
实验吧 CTF 习题：链接
XCTF OJ，链接
南京邮电大学 CTF/网络攻防训练平台，链接
HackingLab 网络信息安全攻防学习平台，链接
CTFLEARN，链接
Jarvis OJ，链接
pwnable，链接
渗透测试演练系统 OWASP_BWA、DVWA、Mutillidae、Web for pentester
渗透测试靶场、平台红日攻防汇总，链接

CTF Writeup（过程）：

CTFs Writeup 集锦，链接
CTF writeups from P4 Team，链接

```
补充：网络安全法解读，视频链接
```

6 一些学习网站、课程

```
学习网站之 i 春秋，链接
学习网站之安全牛课堂，链接
学习网站之中国大学 MOOC，链接
学习网站之网易云课堂，链接
学习网站之慕课网，链接
学习网站之 PHP 中文网，链接
一些课程之大学计算机专业课程体系，链接
一些课程之 i 春秋职业体系课程，链接
一些课程之 Web 安全微专业（前置课程）链接
一些课程之 Web 安全微专业（基础）链接
一些课程之 Web 安全微专业（进阶）链接
```

7 常用方法技能

```
CVE 申请报告的编写样例：Report(CVE-2018-11396)
```

8 补充：Web 安全学习过程参考

```
参考文章：Web 安全研究人员是如何炼成的？

相关课程体系、相关书籍
CTF
练习 1：OWASP Broken Web Applications Project，链接
练习 2：hackxor，链接
HackerOne、BugCrowd 难度和回报相对较低的挑战来练手。
资料有：Hacker101 系列、OWASP Testing Guide、《Web Application Hackers Handbook》、《the tangled web》
```

四 安全资料与项目

```
Awesome-Hacking：链接
安全开源项目汇总：链接
OWASP（开放式 Web 应用程序安全项目）：链接，OWASP 中国，链接
OWASP Testing Guide，链接
SECTOOLS：链接
乌云知识库：链接
Paper 安全技术精粹，链接
All conferences and series，链接
kitploit 黑客工具介绍，链接
connect-trojan（Remote access trojan）：链接
Web 安全相关的技术点，链接
经典的挖洞过程，链接
CTF 学习资源，链接
pwnable 小游戏，链接
Payloads and bypasses for Web Application Security，链接
红日攻防资料汇总，链接
信息安全知识库，链接
routerpwn，链接
Embedded Device Hacking，链接
rootkit analytics，链接
```

五 安全工具

信息安全导航站：安全圈之安全工具
安全工具红日攻防汇总：链接
1 威胁情报

```
RISKIQ，链接
cymon，链接
华为情报查询，链接
绿盟威胁分析中心，链接
360 威胁情报中心，链接
启明星辰威胁情报中心，链接
Alice 威胁情报溯源平台，链接
REDQUEEN，链接
微步情报社区，链接
```

2 文件分析

```
virscan，链接
腾讯哈勃，链接
virustotal，链接
微步云沙箱，链接
百度 WEBDIR，链接
malshare，链接
vicheck，链接
```

3 网站检测

```
百度安全指数，链接
腾讯御知，链接
360 网站安全，链接
ZMap，链接
```

4 APP 漏洞与恶意分析

```
360 显危镜，链接
腾讯金刚，链接
腾讯在线查毒，链接
爱加密，链接
爱内测，链接
通付盾，链接
```

5 Web 大数据

```
钟馗之眼，链接
FOFA，链接
shodan，链接
censys，链接
傻蛋联网设备搜索系统，链接
scans，链接
谛听，链接
```

6 其他工具

```
漏洞搜索引擎 sploitus，链接
1/nday & Exploit（Metasploit 漏洞利用），链接
Public Database Directory - Public DB Host，链接
站长工具，链接
查企业，天眼查、启信宝
注册过哪些网站，链接
Google Hacking Database，链接
全球 DNS 搜索引擎，链接
在线 XSS 扫描，链接
```

六 信息安全咨询与信息、期刊、论坛站点

信息安全导航站：安全圈之安全站点

1 信息安全咨询与信息

```
Hacker News，链接
FreeBuf，链接
安全客，链接
安全头条，链接
SecWiki，链接
被黑网站统计：链接
```

2 安全期刊

```
安全客周报与季刊，链接
360 研究报告，链接
瑞星周报，链接
SecWiki 周刊，链接
```

3 相关论坛站点

```
吾爱破解，链接
看雪论坛，链接
红日攻防实验室，链接
i 春秋，链接
暗安全技术小组，链接
Offensive Community 论坛，链接
cracking 论坛，链接
pentester，链接
安全牛，链接
雨苁，链接
```

4 推荐关注的组织与个人

```
YouTube 关注：

Black Hat
Bug Bounty Public Disclosure
Bugcrowd
CernerEng
DEFCONConference
HackerOne
hacktivity
OWASP
```

七 安全会议与会议资料

```
BlackHat
DEFCON
安全会议资料：链接
```

八 安全感知

信息安全导航站：安全圈之安全感知

1 态势 CyberMap

```
百度安全指数之互联网指数，链接
kaspersky，链接
华为态势，链接
fireeye，链接
akamai，链接
fortiguard，链接
云堤 DDoS，链接
```

2 SRC 应急响应、漏洞报告

```
EXPLOIT DATABASE，链接
CNVD 漏洞平台，链接
信息安全漏洞门户，链接
知道创宇 Seebug，链接
安全联盟，链接
乌云，链接
360 网络安全响应中心，链接
教育行业漏洞报告平台，链接
国家互联网应急中心，链接
国家信息安全漏洞共享平台，链接
其它，参见 安全圈之安全感知
其它 SRC 应急响应
```

3 众测

```
360 众测，链接
阿里云先知，链接
漏洞盒子，链接
看雪众测，链接
sobug，链接
CNVD，链接
bugcrowd，链接
hackerone，链接
```

九 一些安全企业、行业全景图

```
参考：安全牛，网络安全行业全景图（2018年7月）发布

一些安全企业：
一些安全企业

安全行业全景图：
安全行业全景图
```