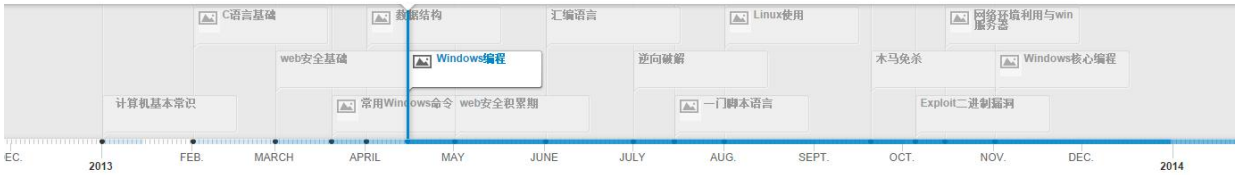
【西电信安协会-技能时间轴】-【20140917】



最近西电信安协会的技能轴更新了，这是老版的，我觉得更接地气

注意，这十五个知识快可以组成几条不同的学习链路，然后基本上涵盖了信安主流的各个技术方向。当然知识体系不全，比如没提到PHP和MySQL。
但是注意学习周期，比如1的基本常识，上边有个日期“January 1, 2013 — January 15, 2013”，算下来就是15天的学习周期。这个周期是西电的同学针对无基础，有大量课程的本科生指定的，咱们虽然也有实验室任务，但起码要折半吧。

在信息安全人才如此急缺的情况下，扎实的计算机、网络综合基础知识是前提，安全素质才是我们的核心竞争力。

1、计算机基本常识

January 1, 2013 — January 15, 2013

计算机基本常识

了解计算机基本常识，常用软件使用。

需要学会基本使用的软件或技术有：Word、VMware、VPN、Visual Studio、FireFox及其插件、一款编辑器，学会如何截图、编译运行程序、使用Google查询资料、邮件列表加入与收发。

2、C语言基础

February 1, 2013 — June 1, 2013

C语言基础

学习基础的C语言，不管是否是编程方向，我觉得都有必要了解一些C语言，会编写简单的C程序代码。

推荐的入门书籍有：谭浩强《C程序设计》、《C和指针》

C语言对于初入门的同学来说是一座大山，但一旦翻过了这座大山，前面将会是一马平川。如果想深入研究C语言，《C和指针》这本书将是你最好的选择。

3、数据结构

April 1, 2013 — June 1, 2013

数据结构

开发方向的同学必学，其他方向的同学也可以适当了解。

在C语言学习到一定阶段后，可以开始了解数据结构，它和C语言相辅相成，可以说在我们学习C语言的后期，很好的对我们C语言知识进行了整理。当学习完成数据结构后就可以写一些ACM的竞赛题目了。

推荐郝斌老师的数据结构教学视频。

4、Web安全基础

March 1, 2013 — May 1, 2013

web安全基础

了解web应用的各种常见漏洞（知道是什么，如何形成）：SQL注入、XSS、CSRF、上传漏洞、解析漏洞、任意文件包含漏洞、点击劫持、弱口令、cookie欺骗等，
会使用一些常用入侵检测工具和辅助工具，并入侵一些安全系数较低的web应用。

了解关于web安全的周边知识，如：能判断某密码的hash类型、能识别一些常用的web指纹、能在互联网上搜索目标相关信息、了解一句话木马并会利用等等。

5、常用Windows命令

March 20, 2013 — March 31, 2013

常用Windows命令

做渗透的同学，尤其需要首先学习一些常用的windows命令(最好在实战中边运用边练习)，特别是入侵检测是常用命令，如net user、net localgroup、net use、net share、net start、arp、whoami、regedit、tasklist、find、cp、mkdir、del、dir、print.....

提高：能写一些批处理脚本，完成一些重复性任务

6、一门脚本语言

July 15, 2013 — October 1, 2013

一门脚本语言

对于做渗透测试方向的同学尤为重要，对于做开发的同学也可以学习一门脚本语言。

我推荐的是python或php，学习python可以快速开发出一些有针对性的脚本，而学习php可以尝试进行web漏洞的挖掘。

7、Linux使用

August 1, 2013 — December 1, 2013

Linux使用

学习渗透的同学在这段时间又能分为两条路，一是web安全，二是内网渗透。web安全偏重于web应用漏洞挖掘和利用，内网渗透偏重于网络环境的分析、内网计算机的漏洞利用。

内网中大部分重要计算机属于Linux，所以学会Linux基础的使用，Linux各种服务的搭建、维护、漏洞利用修补是必须的。

推荐图书：《鸟哥的Linux私房菜》

8、Windows编程

April 15, 2013 — December 31, 2013

Windows编程

在数据结构学习完成之后，我觉得就是一个分水岭了。做渗透方向的就不必继续深入Windows编程，大可继续积累网络安全经验，但开发、逆向的同学就需要学习windows编程了。

Windows编程无非就是阅读MSDN，熟悉每个windowsAPI的用法，平时想到的好点子可以尝试写成程序，增加自己的代码量积累。

windows编程也是一个积累的过程，需要慢慢了解每个API，所以学习起来并不紧张。

9、Web安全积累期

May 1, 2013 — December 31, 2014

web安全积累期

其实积累是一个长期的过程，所以也不分期限的。平时可以在如90、法客、土司、乌云、习科之类的安全社区和大家一起讨论，多关注最新的技术、漏洞，平时注意搜集每个漏洞的成因、利用方法、修补方法，并尝试在网上寻找实战的机会。

这段时间还可以学点脚本语言，当掌握了一门顺手的脚本语言后就能更快速、更便捷地做很多针对性的攻击。

10、汇编语言

June 1, 2013 — September 1, 2013

汇编语言

汇编也是一门基础课程，对以后的逆向破解、漏洞挖掘、木马免杀的学习都有直接影响，在windows编程的学习期间可以开始学习汇编。

大概了解16位的汇编语言，知道基本语法，重点在32位汇编的学习上。学习汇编语言可以结合自己写的C程序，将自己写好的程序调试，单步调试每一句汇编语言，不懂就查。

11、逆向破解

July 1, 2013 — October 1, 2013

逆向破解

在汇编基本语法学习完毕后，可以选择性地开始学习逆向、破解相关操作。

在学习逆向的过程中就可以熟悉之前学习的汇编指令的使用

推荐图书：《加密与解密》

12、木马免杀

September 20, 2013 — March 1, 2014

木马免杀

在逆向学习完成后，又可以分为几个小方向：深入破解、exploit、木马免杀。

能够自己编写木马后，最需要的就是免杀。如果编写的病毒木马不能运行，也无济于事。免杀成功与否是运气、经验、灵感、技术、耐心的集合体，缺一不可。所以虽然很多人尝试学习，但最后真正能做到完美的人并不多

推荐图书：《黑客免杀攻防》

13、网络环境利用与Win服务器

October 15, 2013 — February 1, 2014

网络环境利用与win服务器

在Linux基础学习到一定程度后，可以开始学习网络，如何利用内网内各种计算机开启的各种服务，来达到渗透进目标机器的目的。

当然，同时也要学习Windows服务器的使用，了解什么是域，如何在windows环境下使用各种服务。因为一个大内网下一般个人机、目标机是windows系统。

14、Exploit二进制漏洞

October 5, 2013 — April 1, 2014

Exploit二进制漏洞

在逆向学习完成后，又可以分为几个小方向：深入破解、exploit、木马免杀。

其中Exploit对技术要求较高，回报也最丰厚，所以是很多大牛集结之地。学习exp需要对C、C++有牢固的基础，并有一双发现问题的眼睛。在他人眼中可能只是一个软件崩溃或错误信息，在exper眼里就可以是无穷无尽的财富。

15、Windows核心编程

November 1, 2013 — May 1, 2014

Windows核心编程

在Windows编程学习到一定程度后就可以开始核心编程，其实二者并无太大区别，只是核心编程更加偏重windows内核的一些机制。当你的技术不仅限于开发桌面应用以后，木马、病毒这些更接近系统底层的东西既可以满足要求。

这本书对于以后做开发的同学必看不可：《Windows核心编程》、《天方夜谭》、《寒江独钓》