桌子上放着许多海报

描述已自动生成

最近浏览了灰袍推送的tg频道，记录一些有意思的言论。灰袍推送中有些关于方法论、工程化、区块链的东西很有让人眼前一亮的感觉在此记录一下，方便以后查看。

## 来自@灰袍推送

* 论黑客工程化是我们的追求。黑客工程化是我们的追求。黑客工程化的意思是：我们的所有技能需要成体系活动，能交给机器的都交给机器，我们控制机器“木偶们”来加速我们的效率。为了最优这个工程化，我们很明白什么技能是必须精通的，什么技能是够用就好，什么技能是拿来主义。
* 那个“安全技能树”圈子，新人太多，我一旦分享点复杂的，似乎都安静了。对于陌生的知识怎么办？先 mark，以后有机会再消化，没机会也无所谓，至少知道有这个就好。对于不陌生的，赶紧跟上实践。实战派，不废话。指的就是这个。
* 灰帽 C#，这本书很不错，玩 Win 渗透的，建议这本书实操完。
* 什么黑客技术是好技术？黑产或 APT 组织已经在实战的技术 。
* 很多人不明白什么是职业什么是业余，什么是兴趣什么是工作。举个例子，黑客攻防，是我兴趣，也是工作，更成为了职业。而玩玩比特币、打打王者荣耀、吃吃小龙虾虽也是兴趣，但很业余，我不会通过这种方式去赚钱，能赚到也是投机罢了，如果能成大事，那也是投机，命运选中了我而已。再往细了说，黑客攻防分支领域几十条，也仅某些条会是我的职业，而有不少仅仅是业余，如打 CTF、玩黑手等。
* 通读两本行业一流的书籍是最稳的入门进阶方式。
* 设计一个商业模式的快感大于设计一个软件工程，不过都小于挖到一个大 0day，因为大 0day 自带牛逼的商业模式😄。
* 那些老协议，没认证与加密设计的，都会出大问题，多个 S 多关键。<https://rtpbleed.com>
* 天天喊发干货的人，我就问你 Kali 的每个工具你都了解过没，哪怕绝大多数点开看看都没吧？都懒成这样，是懒还是蠢？
* 干货拿走，消化一年再说：<https://github.com/coreb1t/awesome-pentest-cheat-sheets>
* 钓鱼攻击类型我总结几类：普通域名钓鱼、双因素钓鱼、XSS 高级钓鱼、CSRF 高级钓鱼、浏览器扩展钓鱼、系统木马钓鱼、MITM 钓鱼。这些细节在我的硬盘里。
* 建议大家开始关注“区块链”技术，在自己的技能树上多一个这个是好事，至少可以很好避免成为投机者中的韭菜。玩安全的，可以探索这个领域的安全问题。
* 不小心连续发的都是区块链相关的观点。做安全就是这样，需要跟上时代。区块链安全里，我们会把其分为两大类：区块链本身的安全，区块链之上各类业务的安全。对于我们来说，区块链本身的安全是我们的技能短板，里面大量的安全问题是需要算法、架构、工程的整体思考。如果不能深入到区块链创造细节里去，这类的安全从何研究？
* 未来的世界是去中心化与中心化的博弈平衡，绝对不会有完美的去中心化生态，原因请自行阅读《自私的基因》...
* 安全研究第一步：**目标攻击面**都有哪些？第二步：**攻击路径如何描绘**出来？这两大步骤是最考验安全人员经验及想象力的地方。
* 区块链世界最伟大的点在于：通过技术信仰吸引一批信徒且都利益绑定了。
* 比特币网络新增两个杀手锏，一个是闪电网络，一个是 RSK。
* 《麻省理工科技评论》2018 年“全球十大突破性技术” ：[http://mp.weixin.qq.com/s/\_kdbSRdIwr4bIXfNtut8Fw，匿名货币Zcash在十大之一里被提及。](http://mp.weixin.qq.com/s/_kdbSRdIwr4bIXfNtut8Fw%EF%BC%8C%E5%8C%BF%E5%90%8D%E8%B4%A7%E5%B8%81Zcash%E5%9C%A8%E5%8D%81%E5%A4%A7%E4%B9%8B%E4%B8%80%E9%87%8C%E8%A2%AB%E6%8F%90%E5%8F%8A%E3%80%82)
* 看到 bettercap 从 Ruby 改为 Go，就等着 MSF 和 BeEF 了。黑客工程化的世界，要么 Python 要么 Go，其他都是小众，JavaScript 还差些火候。
* Google 说了“您应始终使用 HTTPS 保护您的所有网站，即使这些网站并不处理敏感的通信。
* 你猜为什么？尤其是那些区块链世界的网站，即使上面没 Web 钱包，没交易所功能。
* DNS Rebinding 技巧用于钱包节点 HTTP RPC 的攻击确实很猥琐，上古时代的技巧到现在还是这么的帅！
* DNS这种设计一直是信息安全头顶的一朵乌云。

文本

描述已自动生成

* 当年门罗币背后的那些人设计出这个币种时有没有预见过，这个举动无意间让网络世界和平了不少:-)
* 一次漂亮的分享最大的利己是：极其加深自己对所分享知识的印象。
* 一个好漏洞从发现到 PoC 到 Exploit 到 Attack 到 Defense 到披露，可以完美打通一次任督二脉。这样的机会不多，多珍惜。
* 过了遍比特币生态网络里的 RSK 生态解决方案及相关源码，他们对安全有不错的理解，尤其是他们应该早有意识到以太坊生态安全缺陷，这点很赞。
* 以太坊智能合约的出现让软件工程师真的可以对得起工程师称号，多好的事。
* 创业最爽的是还能亲自带队攻克两个核心能力：1. 0day；2. 黑客工程。
* 玩前端黑只需掌握 Chrome DevTools 就好:-)
* 区块链本质根本不是什么去中心，而是利益共识。明白这点就行了。而我是游走在两个极端之间的人，我只知道这里存在很多安全攻防博弈。乱，浮，和你我无关，我们改变不了。
* 最快的成长方式就是实战中成长，比如你拿到攻击者的样本，立马可以吸收其手法精髓，防御上就可以有的放矢。再比如为了突破，你死磕到底，一回头会发现：卧槽，掌握了各种技巧，而这许多是死磕前绝无法想象到的。
* 创造比纯粹的 Hacking 更重要，但 Hacking 才能促进更独特的创造。
* 探索本质这是黑客必须具备的基本素质。
* DApp 游戏本质是一场“代码即法律”的黑客游戏。
* 黑客的初阶是逆向思维，进阶则是正向思维。
* 区块链领域的黑客几乎都不是曾经的黑客，他们几乎都是很懂区块链的技术人员，且带了点逆向思维。曾经的黑客几乎都过时了，绝大多数没机会在这个新领域开天辟地，只能费劲地跟着。
* 5G 与 IoT 时代的风险与机遇：<https://threatpost.com/the-danger-and-opportunity-in-5g-connectivity-and-iot/138493/> 如果 IPv6 也大量启用，那对网络空间测绘来说，是个新挑战🤔。
* 我说我们在做区块链安全，其实我们在做都是公链生态的安全，慢雾的机会仅在这，如果这个生态没了，慢雾也会沉静甚至消失。是的，所谓的联盟链、私链不是我们的机会，我们的机会在自由的网络空间里:-)
* <https://mp.weixin.qq.com/s/s-gxfYsGUeosiRwpXoWN6w>
* 维基解密新年推文里问：2019，你认为哪些被泄露的档案最能改变我们对人类文明的理解？... 要搞大事？

## 来自@****Ton&OKEx中文频道****

Ton区块链继承自Telegram，旨在为数十亿用户提供服务。它拥有超快的交易速度、低廉的费用和易于使用的原生应用程序，其中一些应用程序可以直接在Telegram中使用，如 @wallet 或 @cryptobot 。