20210130-周报总结

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **小论文进展：** | **🞎阅读文献** | **🞎做实验** | **🞎撰写中** | **🗹其它** |
| **一、本周工作**   1. 《网络安全现状与未来蓝图》看了下从业人员对网络安全的现状的判断。 2. Python还是继续复习，突然发展十进制浮点数的处理，都使用decimal 模块，看看有没有其他方便的方法。 | | | | |
| 1. **下周计划** 2. Python试试写个程序，实践一下，看能不能有点什么小效果。 | | | | |
| 1. **本周工作摘要**   世界走向数字化，现在的世界空间已经完全可以按照物理（Physical）和非物理的(cyber)来划分了。  其观点是“意识是第一位”有严重问题的基本都是意识出问题了，不是技术出了问题。    4攻击方和防御方的对抗视角  要想做好网络安全防御，就要站在攻击方的视角看问题，网络空间HK惦记的就是你所守护的，沈院士描述的霸权国家、敌对势力、黑客组织和你所守护的对象防御程度成正比。 攻防对抗的视角 1寻找漏洞和减少目标暴露面  其实攻击者也很累，如果攻下来的目标价值不大甚至被反制，攻击者也会很郁闷，浪费时间和心血也是很耗功力的，初学者会因为兴奋而攻击，老炮们要是没有激励和内在动力。其实也不愿意熬夜了，拿下目标的瞬间荷尔蒙飙升、圈子里的扬名、财富以及为组织增光是主要激励，所以寻找合适的有价值的目标是攻击者的前提。  对于防御者来讲，就是了解自己保护的对象对黑客的吸引力，尽量减少暴露面，IP,端口，服务，主机名，操作系统、支撑软件，web服务，不是自己必要直接外露的，能减少就减少，能在深宅大院，就不要在街口开门。  2信息收集和反信息收集  对于攻击方来讲，目标确定后会通过各种方式进行信息的收集，可以采用社工的方法收集关键人的互联网喜好和惯用的工具等等，也可以仅仅是IT信息，信息越多攻击者就可以结合使用，对于高级目标，几个月到半年甚至更长的时间，一点点收集。  对于防御者来讲，自身个人的信息，守护对象的信息、外包商服务商的信息、采用的IT系统的信息、暴露面的信息，入侵监控的信息，都是需要保护的和提高警惕的。  3找弱点和减少弱点  对于攻击方来讲找弱点的方式，最简单最暴力最直接的就是采用大型扫描器，分布式扫描器，一个目标的地址段暴露面都是弱点集中的地方，往往一次大规模的漏洞爆出，就是找到弱点最简单的办法。不管是网络层的、系统层的、应用层的还是弱口令的。这些简单弱点就是入门第一选择，当然，Oday另外再说。  对于防御方来讲如果平时的弱点管理的好，及时更新，动态监控做的好还可以，往往弱点的爆出没有及时的采取措施，很可能在这个时间差就已经被侵入了，实践经验中弱点的管理需要交叉异构。我们做了一个站在甲方视角的弱点管理平台，效果确实还是不错，曾经出现的一起事件，某盟的弱点管理发现了问题，但由于操作系统厂商已经没有了，虽然也发现了但没有预警，其实甲方还在大量的使用此操作系统，交叉使用的弱点管理平台起到了很好的效果，预防了一次较高级别的APT攻击事件(两会期间)。  4强盗式进门攻击和第一道防线  DDOS用的越来越少了， 主要是太野蛮也暴露的太快，现在的云服务商、运营商都已经有很好的防护了，加上监管单位打击，这种方式确实实用效果一般。现在强盗式攻击反而采用字典爆破成为主流的，验证码绕过的也不少，12306经受了多少次的洗礼，特色的验证码就是证明，这个领域的防护说起来一点都不难，但这个领域出问题的也是最多的，可以说无知者无畏。总结几点线守则，对外服务的系统甚至内网的系统，多重验证是非常必要的，安全策略加大强制弱口令不得生存，关闭不必要的服务、端口和清理root账号。软件开发商稍微懂点按照安全软件编程开发和防范，其实就这些，一个系统这里的投入不会超过几十万就基本可以安心了。  5温柔式内网攻击和第二道防线  静默型攻击从08年以后就是主流了，大规模的炫耀式的病毒攻击基本消声觅迹了，都已经悄悄地进入打枪的不要，APT、APT、APT是我们天天防护的重点。就如我上文所说，攻击者也很累，现在没有人愿意敲锣打鼓的去说我要攻击你，更多的就是低调低调低调，第一道防线被撕开口子的概率是比较大的，一但进来如果防御者做的好，攻击者就是进入深渊的开始，每个不合适的内网嗅探，试图提权，异常行为，其实很好抓。我们现在总结出来经验，基本上进来的APT跑不了，要不不敢动，一动就会发现。总结几个关键点，全网全流量监控，全网主机系统监控，控制好有限的特权用户/普通用户账户并进行行为监控，安全域策略最小化原则并动态可视监控，在核心主机和数据系统里做好黑白名单的可信验证。一点也不高深特简单，不用PPT吹NB，做好落地了基本保证第二道防线没问题。我们把这些统合起来做了个系统，称为防御平台核心检测功能，现在用了的客户都没有被HW干掉，实施一个满意一个，我们也特别有成就感。这个估计未来会成为主流的趋势，实干简单清晰化防御体系里的检测系统，感谢PCSA联盟的KL,QT,ZX,SBR,ABT，CT,ZR，kx (科来、青藤、中新、圣博润、安博通、长亭、中睿、可信….)安全能力者们。你们做的探针真的很NB，也确实是未来的安全中间力量，和品牌没关系，要看能力，真安全未来大浪淘沙。 | | | | |