复盘攻防，再聊安全

Cnrstar 四维创智 今天

截止到28日5点，HW行动终于结束，朋友圈感觉是在过年，到处是倒计时和庆祝声。看来防守方们7*24小时的看监控还是比较无奈的。本次复盘基于我对整个护网行动的观察总结而来，仅代表我个人观点，如有不妥之处，欢迎交流。

1 整体攻防的思考

本次攻防，从规则到各方实力，都是绝无仅有的。经常有人问，是攻击队厉害还是防守队厉害？经过我这些年的思考，还是没有得出一个确切的结论。有时候觉得攻击队厉害，因为攻击可以在非特定时间随意发起，出其不意攻其不备，甚至手持0day指哪打哪，毕竟木桶原理决定着攻破一处即可内部突袭；有时候又觉得防守方厉害，因为防守方拥有全部访问流量，随时洞察攻击者的探测并封堵IP，也可以在主机层监控攻击者一举一动，甚至部署蜜罐玩弄黑客于鼓掌之中。总之，这么些年的摸爬滚打经验告诉我，攻防就是这样，道高一尺魔高一丈，一如黑客防线中说的“在攻于防的对立统一中寻求突破”。

2 从攻击方思考

在真实的攻击行动中，一般一个目标要搞到核心系统根据防御程度不同，也需要1个月到半年的样子，甚至APT要潜伏一到两年才能拿到自己想要的数据。而此次总共给攻击方的时间只有3个周，并且每个队伍据说10多个目标，这也就决定了攻击要快速、要自动化。

a.分布式扫描器

要说快速，还是得上扫描器，但是一个扫描器速度肯定不行，再者，被发现攻击行为，立马IP被ban掉，后续就无法进行。所以，分布式扫描器在这种情况下一定是个趋势。首先对全部目标的全端口进行一次扫描+端口识别，根据Banner快速收割一波；

在这个过程中就会有个坑，比如在收集二级域名时，经常采用字典爆破，而防守方会设置一个诱饵二级域名，把流量引入蜜罐之中，坐等上钩。这就需要攻击方们机灵一点，时刻反思这个是不是蜜罐，至于怎么发现蜜罐，以后再聊。

对于AWVS的扫描器，还得请各位升级到最新版，别被防御方反制，毕竟老版本扫描器自身就存在一个RCE。

b.菜刀？蚁剑？冰蝎？

对于所有的黑客来说，菜刀肯定是一个传奇，一直是最稳定、最牛逼的webshell管理工具之一，但是同时，菜刀也是一个最容易被发现的攻击工具，毕竟流量特征太明显了，而且一旦发现就100%意味着服务器已沦陷，防守方会里面下线进行深入分析。说起来菜刀好像是11年左右发布的（如有记忆偏差，请指正），还记得当初第一次见到这工具时的感觉，那感觉总结起来就是一句话，“卧槽！牛逼！”。因为在菜刀之前，我们学习的都是先小马后大马的姿势。而用了菜刀之后，我深刻理解了什么大马小马都无所谓，能执行命令搞定目标的都是好马。然后经过了几年的迭代，中国菜刀在国内安全圈也是经历了各种风风雨雨，各种后门版满天飞。最后鉴于其加密性能较弱，陆续出现了几个替代版本，蚁剑就是很优秀的一个项目。讲真，我开发水平相对较弱，见到蚁剑才发现原来js也可以写出优秀的跨平台客户端应用。可是正式由于其nodejs写的，才导致其跟AWVS一样，存在一个本地nodejs解析的RCE，很可能被防御方反制。再之后给我“牛逼”感觉的就是冰蝎了，其双向通信加解密的管理方式，让诸多基于黑名单正则的防御产品厂商直接歇菜。可是很奇怪的时，还是有很多大量攻击方采用菜刀、jspspy之类的原始webshell，结果被防御方轻松发现并清除。

不过说到最后，我有一个疑惑，为何大家非得用webshell这种方式搞服务器呢？比如在存在weblogic反序列化或者Struts2 RCE漏洞时，黑客们写的工具还是一键写入webshell这种。安全发展到今天，防御手段越来越多，各位白帽子是时候改变了。正如我之前说的，不管用什么shell工具，只要能在服务器端执行命令，下面就肯定有更好的解决方案。我一般会使用命令方式加载自己的二进制版远控来操作，现在的二进制远控，不像以前，还得生成exe用菜刀上传，在命令行下执行，现在基本都可以做到类似mshta或者powershell的一句话直接动态上线，并且基于TCP/UDP协议的命令执行、文件管理，一是稳定，二是完全绕过那些基于黑名单的流量分析设备。类似metasploit的脚本payload反弹的meterpreter，但是msf特征明显，也容易被杀，所以我个人估计后面攻防还是会发展到类似cobalt strike之类的工具对抗上。

c.水坑&鱼叉

针对水坑或者鱼叉攻击来讲，可以想象到肯定大量的攻击队伍采用这种方法进行攻击，攻击手法多基于邮件进行。现在假想成攻击队伍，我会首先在github上搜索一波，举个例子：https://github.com/search?q=%224dogs.cn%22+password&type=Code，注意域名要加上双引号进行精准匹配。在翻到一个可登陆的邮箱后，去通信录导出所有联系人方式，进而进行简单的口令爆破；在这些操作还没拿到有用密码的情况下，就可以根据组织结

构进行定点攻击了。高级点的用浏览器0day，没0day的也可以直接发宏病毒，注意编个理由加个密发，防止被沙箱抓样本。

假如没有有用的邮箱账号，也可以搜索引擎收集一波邮箱，再根据明明规则，加载中国姓名top500字典进行组合，总归能抓到一两个用弱口令的。

如果还是啥都没有，也可以使用swaks之类的直接伪造成admin发送钓鱼邮件。至于发送内容和技巧，以后再聊。

对于防御方来讲，最厉害的莫过于直接关停外网邮箱了。次之，可以派人随时查看登录日志，及时发现异地登录爆破情况。对于有钱的甲方爸爸们，可以通过流量镜像，对附件进行沙箱判定。

d.内网渗透，还是要了解业务

在突破边界进入内网后，剩下的主要是内网渗透了。内网渗透可以简单分为横向渗透和纵向渗透。内网渗透的实质和关键是信息收集，通过不停的突破系统拿到更多的权限，而更多的权限带来更多的信息，最终在信息和权限的螺旋迭代下，拿到目标的最高权限。

对于有域的环境，一般目标时拿下域控，而在本次攻击中却恰好爆发了一个直接打域控的0day，这就容易多了。但是即使一键拿下域控权限，还是要回到信息收集的本质上，要在海量的终端里筛选出自己的目标数据在哪台机器里，还是需要一些技巧的，展开来讲，有空再聊。

而不管是什么环境，我个人感觉阻碍攻击队伍进行内网渗透的主要原因还是对目标业务的了解程度。比如电力行业的16字方针（此处略），很多时候搞到边界系统后，ipconfig一看是10段的，以为进了个大内网，而实际情况是那只是冰山一角而已。纵向突破还有很长很长的路要走。再者，假如对电信行业、金融行业不了解，进到内网肯定也是一脸懵逼，一副“我是谁？我在哪？”的感觉。这也是内网渗透耗费精力的原因。

e.0day的优劣势

在本次演习中，陆续发现了大量的0day，印象里不完全统计有七八个，具体0day细节可以参考各大公众号之前的报到。这里只讨论下针对0day的问题。

从0day的内容和数量上来讲，护网结束后我是看啥系统都有漏洞，并且有一种想去挖几个留着的冲动，奈何工作杂事太多，先搁置一下吧。

对于攻击方来讲，手握0day是指哪打哪的一个有效支撑。从漏洞类型上，基本覆盖web、网络、操作系统等等方面。针对国内的网络安全现状，讲真，我对那些商业应用真的不报任何安全的奢望。对于国企和政府来讲，自有系统大都是外包厂商开发，而这些外包开发者，大概率不懂安全，甚至sql注入是啥都不知道，更别说防御框架漏洞了。所以对于攻击者来讲，去攻击一个客户广泛的厂商，拿到一个0day即可攻下其相关的所有目标，收益非常高。但同时也要明白，现在0day的生存期非常之短，10年前，我们一个0day可以用半年都没被人发现，而在这次演习中，0day的生存期可能只有半个小时，因为防守方发现shell就会溯源，进而预警。不过排除这次防守方7*24小时的有效监控，在真实情况下，0day的生存周期可能不超过一周。所以，我认为，当前网络环境中，0day大量存在，但使用非常谨慎。至于防守方怎么防御0day，请看后面内容。

3 从防守方考虑

整体来讲，防守方都是从“事前排查”、“事中监控”、“事后溯源”三个方面进行防御的。根据我的观察，普遍来讲，国企安全防御能力弱与互联网公司，而相反，国企和政府单位的投入普遍高于互联网公司。这也就导致了演习前大量的“人贩子”到处求人驻场的问题，一度炒到人天上万元。下面从几个方面分析这次防守方的经验和教训。

a.防御过度问题

至于这次演习的意义和重要性，各位甲方自己应该更明白，这里不再描述。而正是由于防御方的重视，所以出现了大量的防御过度现象。一是在开始前的大量系统关停，二是对于互联网IP的大量封禁。首先大量的关停本质上类似掩耳盗铃一样，在护网结束后依旧面临各类外部攻击者的威胁。希望存在这类情况的厂商，还是能从根源上排查漏洞，加固系统，对系统采取必要的防护措施。

针对恶意封禁IP的情况，虽然体现了防守方及时发现攻击的能力，但同时，也实实在在的影响了正常业务的运行。特别是一封一个B段的情况，我表示可以理解，但也不忍直视。同上，各位甲方还是考虑下从根源解决问题。

b.应急排查

对于事前的应急排查，甲方大都采用临时购买人工渗透服务的方式进行，而毫不客气的说，你们买到的有一部分却是在校大学生，或者培训机构的实习生。即使钱给够了，去的是个渗透大神，也会因为内网漏洞太多，无法完全覆盖。以我个人举个例子，假如给我一个系统，我大概需要一上午分析每个端口，每个业务接口的安全性，进而给出一个完整的测试报告，我基本上

可以保证我测试过的系统短时间内不会出大问题。但是假如给我一个B段，告诉我3天完成，那我就只能模拟横向内网渗透，masscan先来一波端口，wvs扫描一波，然后一批一批的去看。这种模式就决定了无法完全覆盖全部业务系统。及时时间够，那对于新增的业务又怎么办？

那针对这种情况该怎么办？我一直给我的客户普及的一个想法是内网漏洞，不要指望短时间内购买一次服务就完全解决了。对于漏洞隐患，工作必须是平时常态化的开展。一是上资产管控手段，对内网所有的服务器，通过主动扫描、被动流量分析等手段进行搜集，实时监控内网到底开了多少端口，每个端口运行什么服务，应用是什么版本；二是解决遗留问题，对内网既有的框架漏洞、弱口令漏洞，进行专项整治。相信通过本次护网，原来没搞过安全的防守方，在部署安全设备后发现了大量的永恒之蓝、木马受控等问题，这些都是遗留问题。建议大家用几周时间集中解决一类问题，循环下去即可解决遗留的全部问题。三是建立新业务上线审查流程，对于新上线的业务系统，必须通过第三方安全测评，只有拿到安全测评报告的才允许上线。

最后，打个广告，我们公司的猎鹰威胁感知系统就是用来做资产管理和大规模漏洞探测，再加上我们的基于AI的渗透机器人，完全可以自动化监控发现各类安全问题。

c.重边界、轻内网的防御策略

这次的防守方普遍是重边界、轻内网防御，造成了一旦边界被破，内网整体垮掉的风险。而这个情况在我入行时就普遍存在。安全发展到今天，实在是说不过去。去年看到了Google提出的0信任网络，感觉是个趋势，一度想转行做0信任网络的布道者，虽然普及还有一段路，但是我还是希望大家可以转变思维，一定一定不要认为我在内网就是安全的。万一哪天被黑，可能影响的就是国家利益，带来的就是社会动荡。

d.威胁情报系统的意义

首先，针对这次攻击，各种原有IOC情报基本无效，比如恶意域名库、恶意IP库等，因为攻击方使用的都是新的域名和IP，这也是黑名单做安全的尴尬。但是同时要感谢安全厂商们的威胁情报库，让更多的国企、政府单位认识到了自己内网办公电脑有很多已经被控制。

e.面对0day攻击的无力感

面对0day攻击，理论上谁都扛不住，但是实际是这样么？仔细想想并非如此，首先，面对0day真正扛不住的是以黑名单为基础的安全设备，包括waf类、态势感知类、IDS类等。而这些安全设备，又确确实实是各大厂商的首选安全监控设备，一旦这些设备没报警，那基本啥都干不了。这也是防守方们7*24小时防守但其实大部分时间无所事事的原因。

首先，对于web 0day的防御，完全可以采用openrasp类防御方法，从根源上防止各类web漏洞攻击。如果有想购买商业版rasp方案的同学，可以勾兑下我哦。

其次，对于网络0day和系统0day，我们可以采用EDR手段进行防御，在终端上装上agent，在agent上采用白名单策略，对于无关的进程启动和危险命令直接报警或阻断。想起来我们四年前做过的一个产品叫麒麟卫士，可以说是国内首款EDR雏形了，可是去卖的时候发现大家对于需要安装agent的做法都耿耿于怀，不敢装。四年过去了，相信后面会有更多的人接受EDR带来的安全改变。

f.蜜罐

这次演习的一大亮点就是很多防御方采用了蜜罐的方式进行诱捕和攻击引流。要说蜜罐做得好，那是真的很有用。我理想中的蜜罐应当是完全仿真，而不是动态针对部分服务的仿真。同时可以具备反制的功能，一是可溯源攻击者真实身份，二是可利用AWVS或者蚁剑这类黑客工具自己的漏洞反向攻击攻击者。相信后面会有大量的优秀产品脱颖而出。不过防守方真的真实部署后，可能半年也捕获不到一次有效攻击，毕竟这次是演习，平时黑客攻击还是少。不过安全就是如此，防患于未然。

写在最后

我个人来讲是一个安全技术爱好者，从攻击到防御，都有涉猎。自从创业以来，干的事情更杂了，但是我一有时间还是在刷安全圈的技术文章，写一些poc。认识我的朋友可能知道，我是一个CEO、一个销售、一个售前、一个产品经理，同时，我也是一个“黑客”，期待着用我的所学所知，能为安全圈带来一些改变。“不忘初心，牢记使命”，与君共勉。


四维创智
专研智能·智汇安全
长按识别/扫描二维码，关注四维创智
官方微信
物联网安全
移动安全
传统安全
四维创智