逐鹿强网，金陵折桂，四届老将0ops战队如何称雄

原创

Cyberpeace 于 2021-11-18 17:12:00 发布 99 收藏

文章标签： 安全 物联网

第四届“强网”拟态防御国际精英挑战赛于2021年11月12日闭幕。本届大赛由中国工程院、江苏省人民政府、国家互联网信息办公室网络安全协调局、科学技术部高新技术司作为指导单位，南京市人民政府、江苏省互联网信息办公室作为主办单位，紫金山实验室、中国网络空间内生安全技术与产业联盟、中国信息通信研究院、南京市互联网信息办公室、南京市科学技术局、南京市江宁区人民政府、南京江宁经济技术开发区管理委员会作为承办单位。南京赛宁信息技术有限公司作为技术支撑单位。

本届比赛共有3018支战队参与线上预选，决出的30支入围战队与18支特邀战队共同参与决赛。比赛历时72小时，最终，来自上海交通大学的0ops战队以263628的得分大比分领先，包揽所有挑战榜单第一，赢得了本届大赛的冠军。

0ops战队是由上海交通大学学生社团信息网络安全协会组织，整合校内著名安全实验室资源组成的团队。目前0ops成员主要是上海交通大学计算机相关专业的在校学生，得到了校直属单位（学校网络信息中心与学生创新中心）和科研团队（密码与计算机安全实验室等）以及腾讯科恩实验室的支持。战队历史成绩包括：第三届强网拟态精英挑战赛亚军、第六届XCTF总决赛亚军、联队取得DEFCON CTF FINAL二连冠等，战果丰硕，实力与经验并存，是一支“拿奖拿到手软”的顶尖高校战队！

“强网”拟态防御国际精英挑战赛组委会对冠军战队0ops进行了联合专访。0ops战队究竟是如何稳坐第四届“强网”拟态防御国际精英挑战赛的“头把交椅”，有哪些“攻防秘诀”可以传授，对拟态防御又有哪些独特的见解，能给未来的参赛选手“打个小抄”？

话不多说，一起来看！

提问一
0ops战队创立的初衷是什么，团队成员组成如何？

0ops战队创立于2013年。当时ACM班的几位学长讨论到国际上新兴的CTF赛事，他们一拍即合，在学校网络信息中心的支持下成立了0ops战队。战队主要面向上海交通大学的在校学生，因此随着前辈们的毕业，战队的主力成员已经换了一批又一批。目前成员主要来自网络空间安全、软件工程、计算机等专业，但也不乏来自机械、生医工等专业的跨界高手。

提问二
0ops战队是参与过四届强网赛的“老将”。与往届强网拟态相比，本届比赛哪些亮点比较吸引你们？

BWM赛制已经成为了强网拟态的经典赛制，但本届比赛中拟态设备的数量之多，是之前几届无法匹及的。新引入的商用设备和ADAS设备也极大地增加了比赛的新鲜感和趣味性，让选手能够接触到常规CTF不会涉及的真实领域。

另外，在前几届拟态赛事中，队里的二进制师傅做完白盒积分赛的题目就下班了，而今年无论是云服务中golang的逆向、还是ADAS的破解利用，都让二进制师傅们有十足的参与感。

提问三
0ops战队实现了四届比赛中的首次拟态设备黑盒逃逸。请谈一下攻击手法，逃逸过程及理解。

考虑到拟态Web服务器的黑盒题目在源码上可能和白盒类似，比赛的第一天晚上我们先尝试申请了拟态Web的白盒，获取到PHP源码进行审计。绕过PHP中设置的限制后，第二天我们依次绕过了三台商用黑盒的WAF，拿到了命令执行权限，于是很自然地把目光转向了拟态黑盒。在拟态黑盒中，有Ubuntu、CentOS、Windows三种执行体。考虑到前两者都属于Linux，在进行一些依赖平台特性的攻击时，他们有可能被同时攻破，使裁决器认为Windows才是异常的那一个。在具体的尝试中，我们发现有大量的PHP函数被禁用，逐一排查漏网之鱼，最后成功实现了文件的写入。考虑到不同执行体的index.html位置可能不同，我们选择对覆盖js文件，通过执行js来修改页面的内容。

事实上，拟态Web的黑盒题目相对其他题目确实容易一些，后来有好几支队伍都实现了逃逸。我们能做到首个突破，可能运气与实力都是很重要的。

提问四
从第一届到第四届比赛，拟态设备不断完善，参赛选手对拟态防御的理解也在不断深入。请谈谈战队对“拟态防御”有哪些理解和看法？

拟态防御是受生物届的拟态伪装现象的启迪而产生的概念，在实际的部署中，分为多台不同系统、不同架构的执行体，以及一台负责分发请求、表决响应的裁决器。通常来说，架构可能采用X86、X64、ARM，操作系统的选择则更为多样。这样的拟态部署对于常规二进制服务的防御是相当好的——由于指令集的不同、随机化地址的差异，让传统的二进制漏洞利用非常困难。

至于使用高级语言的程序，由于高级语言往往追求可移植性，会把系统底层的差异屏蔽掉，让开发者能不受系统差异的影响开发出统一的代码。这种如果存在远程代码执行漏洞，攻击者也可能尝试使用高级语言的特性来同时击破各个执行体，让拟态保护的难度提升。

依据场景，有时还会使用不同编程语言实现同种功能，如今年白盒云平台的赛题使用Golang编写，其API和数据库结构对比去年的JAVA版本是高度一致的。如果在执行体中同时部署多种语言，则能让安全性再上一个大台阶。

最后不能忽视的是，拟态防御难以防御逻辑漏洞，比如一个认证逻辑有缺陷，绕过认证的效果在各执行体的表现都一样，就属于共模漏洞了。这说明应用安全仍然要求代码内部有足够的健壮性，不能完全依靠外部的防御措施。

0ops战队部分队员

提问五
本届比赛首次采用商用设备和拟态构造设备对比测试的模式。请谈谈商用黑盒、拟态黑盒的识别过程、攻击手法。两种设备是否存在攻破速度、攻破手段、识别难度等区别？

在有对比的条件下，才能很好地区分商用黑盒和拟态黑盒，由于拟态有多个执行体，通常来说响应速度会略慢于商用设备。另外对Web应用而言，由于不同执行体的响应头顺序可能不同，多次请求拟态服务器可能也会呈现不同的顺序。至于其他几台DNS设备等，由于能获得的信息量少，确实难以分辨是商用设备还是拟态设备。

至于攻击的难度，看一眼最后留在场上的赛题情况便知：多数商用黑盒早早离场，而拟态黑盒仅有一款被突破。显然想要攻破拟态设备难得多。

提问六
在整个赛程中，是否遇到较为棘手的状况，和无法攻破的难关？聊一下过程。

白盒挑战由于存在注入时间的限制，非常紧张刺激，如果某个环节存在经验不足，很容易无法在时限内完成注入。如银行系统的白盒挑战，我们接连申请了三个回合。第一个回合我们被字符限制所卡住，第二回合又因为不擅长jsp的数据库连接而没能注入，最后第三回合设法连上了哥斯拉，才终于在比赛结束前的半个小时拿下了白盒扰动。

至于其他可以通过白盒拿到环境的黑盒挑战，看下来难度都确实很高，不过由于我们认为领先第二名的分差还足够，所以也没有花太大力气去尝试破解它们（逃

提问七
本届大赛新增ADAS系统及实车验证环节，部署的15款国内外主流商用高级驾驶辅助系统（ADAS）均被赛队选手发现存在安全漏洞。实车验证环节，0ops战队在车内无人的情况下介入商用ADAS系统远程控制车辆。请谈谈ADAS挑战、实车验证环节比赛过程及理解。

几乎每个商用ADAS挑战都存在telnet或者ssh的弱口令甚至是未授权问题，这意味着攻击者一旦攻入车辆内网，就能拿到ADAS的最高权限。除了弱口令，不少商用ADAS设备的端口还存在信息泄露、DOS、栈溢出、命令注入等风险。在新兴领域居然有这么多的传统的漏洞，令人担忧。控制了商用ADAS之后，车辆的总线就在攻击者面前暴露无遗。实车验证的环节又告诉大家，掌握了总线等于掌握了车门、方向、车速等的控制权，这是相当危险的。

提问八
作为四届参赛的“老将”，浅谈参加拟态挑战赛与其他比赛的异同。拟态挑战赛的吸引力在哪些地方？对挑战赛后续的举办（包括赛制、赛题的设置和比赛时间等方面）有什么好的建议？如何才能吸引更高水平的战队和选手来参与？

拟态挑战赛的白盒积分赛和常规CTF比较类似，但其中Web和Pwn题型都引入了一些拟态因素，更有挑战性。此外的黑白盒挑战赛、ADAS挑战赛、还有大家从未见过的巅峰挑战赛都是在其他比赛中绝无仅有的，这些无疑都是非常吸引选手的方面。另外必须承认的是，主办方在奖金上真的非常阔气。

本次比赛客观上也存在一些缺点，首先是各积分分榜无法正常显示，这对各战队的策略规划会起到一定影响。此外，各分项的分数平衡性也值得商榷：一分钟找到一个ADAS设备的信息泄露，等价于白盒积分四道CTF的一血。如果时间精力的付出和分数不成正比，选手会倾向选择更有“性价比”的题目，这虽然可以说是比赛策略的一部分，但是如果因此导致优秀的题目无人问津，那就太可惜了。相信在主办方丰富的经验下，下一届强网拟态赛事会更加精彩。

提问九
作为历经各大赛事考验的一个战队，未来对于战队的发展，有没有什么目标和规划，可以和大家分享一下？

0ops战队的运营规划一直是比较佛系的，毕竟队长和成员们都是在校学生，都有各自的科研学习任务。大家公认的规划就是每年办好校赛和0CTF，在国内每年参加强网杯、XCTF、拟态等等知名赛事，在国际上和科恩实验室等联队打打DEFCON CTF。至于排名，每次尽力不留遗憾就好。另外长远的目标就是希望持续有新鲜血液的加入，希望香火能长盛不衰。

感谢0ops战队带来的精彩回答，也感谢0ops战队在赛场上带来的出色表现！不知道明年将要举办的第五届“强网”拟态防御国际精英挑战赛，0ops战队会以怎样的面貌再次与我们重逢？小编已经提前开始期待了！

第五届“强网”拟态防御国际精英挑战赛，还将有更精彩的赛制、更多高精尖设备、更具娱乐性的玩法在等待着大家。不断升级革新的拟态设备，和不断学习成长的精英战队，最终会碰撞出怎样的火花？

期待我们明年的相遇，也期待更多精英战队继续向拟态防御发起挑战！2022，我们不见不散！