
国内外黑客比赛介绍及对比
IDF实验室
IDF LABORATORY
IDF实验室
www.idf.cn
twitter : @IDF_LAB

关于IDF

?

IDF实验室 简介

- Intelligence Defense Friends Laboratory：互联网情报威慑防御（之友）实验室，简称IDF实验室，是一个民间信息网络安全爱好者的技术俱乐部机构，骨干成员由相关领域的专业人士、技术人员和业余爱好者共同组成。
- 创始人：万涛（我是老鹰）
- 2004-2005年孕育于中国鹰派联盟网，前期以鹰盟网虚拟实验室形式存在。随着鹰盟发展和转型而逐渐转向非营利组织（NGO）。
- 2010年在北京成立实体机构。

关于IDF实验室

- 使命宗旨：

  面向广大信息网络安全爱好者提供计算机安全知识普及教育、参与对业界相关领域产品、发展动态进行客观的、独立的技术、市场研究与评估，为民间信息网络安全爱好者成长为专业安全技术从业人员提供平台和桥梁。

  倡导道德黑客，鼓励安全从业者/爱好者为社会信息化、信息安全化、安全白帽化奉献自己的力量和努力！

- 研究方向：

  互联网威胁发展趋势

  终端安全管理

  无线网络通讯安全

  僵尸网络

安全改变未来

关注IDF实验室

- 网站关注：
  http://www.idf.cn

- 微博关注：
  腾讯微博：@NeteasyIDF
  新浪微博：@IDF实验室
  Twitter： @IDF_LAB

- 邮箱联系：
  idf.lab@gmail.com

概念：夺旗比赛（CTF）

- 夺旗（CTF，Capture the flag），衍生古代军事战争模式，由两队人马互相前往对方的基地夺旗。每队人马必须在保护己方军旗的前提下把敌方的旗从敌方的基地带回自己队伍的基地。

国内部分信息安全竞赛简介

- 2011年上海市信息安全技能竞赛
- 全国大学生信息安全竞赛
- 四川省大学生信息安全技术大赛
- 全国大学生网络安全实战竞赛
- 江西高校信息安全知识及软件设计大赛
- 绿盟科技杯-信息安全对抗技术竞赛
- XCon安全焦点信息安全技术峰会

上海市信息安全技能竞赛

- 由上海市网络与信息安全协调小组办公室主办，上海市信息安全行业协会和上海市信息化青年人才协会承办，上海市信息安全行业协会、公安部第三研究所提供支持。
- 竞赛分为团队运维赛、个人技能赛，参赛对象为政府及企事业单位信息安全工作人员、信息安全行业从业人员及信息安全技术爱好人士。
- 分为资格赛、复赛、决赛三个阶段，其中个人技能赛以基础知识、闯关、夺标等开展；团体运维赛采用技术防御、知识竞答、互动答辩等方式。

- 决赛分上下两个半场，时长共6小时。
- 上半场是选手闯关赛，参赛人员通过发现并清除系统中隐藏的木马、病毒，检测并分析恶意程序样本和应用服务漏洞等，按照闯关等级和时间排名；
- 下半场主要是争夺目标服务器控制权。选手在探索路径进入目标服务器后须检查系统安全性，及时进行漏洞修补、系统修复等工作，以防其他参赛人员利用其他漏洞进入。

上海市信息安全技能竞赛 奖项设置

- 个人技能赛奖项：一等奖一名、二等奖二名、三等奖三名，优胜奖四名。
- 团队运维赛奖项：一等奖一名、二等奖二名、三等奖三名。

全国大学生信息安全竞赛

- 由教育部高等学校信息安全类专业教学指导委员会主办，教育部高教司、工业和信息化部信息安全协调司指导。
- 自2008年起，每年举行一届，每届历时四个月，分初赛和决赛。
- 参赛对象为全日制在校本、专科生。

- 参赛队自主命题，自主设计。竞赛采用开放式，不限定竞赛场所，参赛队利用课余时间，在规定时间内完成作品的设计、调试及设计文档。所有参赛题目须得到组委会认可,并同意后方能参赛。
- 参赛作品开发的软件平台限制为Windows、Linux、Unix。
- 参赛队的参赛内容应该是参赛队员独立设计、开发完成的原创性作品，严禁抄袭、剽窃等行为。

全国大学生信息安全竞赛 奖项设置

- 竞赛设一等奖、二等奖、三等奖和优秀参赛将。其中，一等奖获奖比例不超过进入决赛队伍的五分之一；二等奖获奖比例不超过进入决赛队伍的三分之一。

四川省大学生信息安全技术大赛

- 由共青团四川省委、四川省学生联合会主办。
- 大赛分为初赛和决赛两个阶段。
- 初赛由各高校团委在本校内自行组织。
- 决赛参赛学生必需在规定的时间内进行在线答题和网络渗透，两项成绩各占总成绩的50%，参赛队员完成在线答题后，进入“网络渗透”环节，通过获取比赛设置的铜、银、金三台机器上的机密文件，获得积分，在规定的时间内，积分高的队伍获胜。

四川省大学生信息安全技术大赛 奖项设置

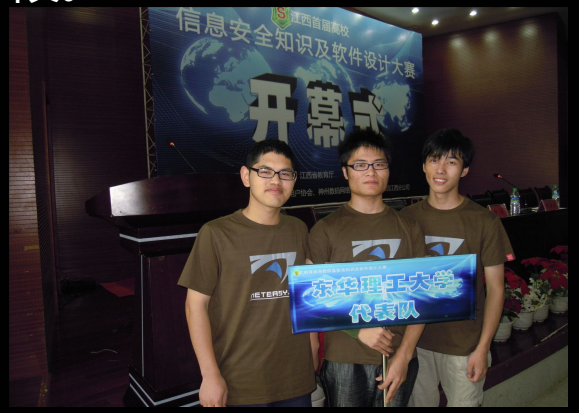
- 大赛分别设置集体奖和高校优秀组织奖。
- 集体奖：设一、二、三等奖和优胜奖。一等奖获奖数为参赛队总数的10%，二等奖获奖数为参赛队总数的20%，三等奖获奖数为参赛队总数的40%，其余为优胜奖。
- 对本次大赛组织工作突出的高校给予优秀组织奖，为参赛高校数的30%。

全国大学生网络安全实战竞赛

- 由天津国家信息安全产业基地、天津海澜德集团主办，西安邮电学院协办，天津云生态信息科技有限公司承办。
- 由各地高校组队（攻击队或防御队）参加地区级别模拟网络攻防实战，分为攻击方及防守方，成绩由监控系统通过自动检测选手成功攻入对方服务次数和保护本方系统正常运行的状态进行评定。获得最佳攻击一方及最佳防守一方的队伍再晋级参加全国网络攻防实战总决赛。

江西高校信息安全知识及软件设计大赛

- 由共青团江西省委、江西省教育厅主办，南昌航空大学承办，IDF实验室提供技术支持。
- 初赛考察学生理论知识，其内容主要包括信息安全技术和网络对抗技术。
- 决赛以网络对抗、网络通关竞赛形式进行，采取包括攻防、对抗、突破内容的实战演练题目，涉及到注入、缓冲区溢出、嗅探、跨站、破解、加解密、信息隐藏、脚本编写等常用计算机对抗攻防手段。



江西高校信息安全知识及软件设计大赛 奖项设置

- 初赛设“首届江西高校信息安全知识及软件设计大赛”优胜奖。另设优秀指导老师奖10名，优秀组织奖10名。
- 决赛设“首届江西高校信息安全知识及软件设计大赛”一等奖1名、二等奖3名、三等奖6名。获奖选手可优先获得相关部门的推荐就业机会。一、二、三等奖奖金总金额为8万元人民币。

绿盟科技杯-信息安全对抗技术竞赛

- NSFOCUS-ISCC：由北京理工大学和绿盟科技公司联合主办。
- 竞赛线上竞技由基础关、脚本关、破解关、溢出关、内核关、真实关六大部分组成。
- 竞赛线下为局域网夺旗模式（CTF）。

绿盟科技杯 奖项设置

- 一等奖1组现金奖励3000元并获得绿盟科技OFFER
- 二等奖1组现金奖励2000元并获得绿盟科技OFFER
- 三等奖1组现金奖励1000元并获得绿盟科技实习机会
- 所有参与决赛环节的学生可获得由绿盟科技认证的获奖证书，并授予“绿盟科技校园大使”称号，决赛选手可获得参加绿盟科技精英特训营的机会。

XCon安全焦点信息安全技术峰会

- 国内最知名、最权威、举办规模最大的信息安全会议之一，在全世界具有一定的影响力。
- 由世界多个国家的信息安全各领域的专家、学者、研究员以及相关专业人士参会，会议以发表演讲为主，演讲议题涉及应用安全、入侵检测和取证分析、无线和Voip领域以及新兴领域的信息安全技术等方面的探讨和研究。

国外/地区主要黑客大赛介绍

- 美国：Pwn2Own大赛/Pwnium大赛
- 美国：Black Hat大会
- 美国：DEFCON黑客大会
- 美国：iCTF国际黑客竞赛
- 美国：FACEBOOK黑客杯
- 韩国：POC安全大会
- 韩国：Code　Gate防黑客大赛
- 俄罗斯：PHDays CTF
- 德国：CodeMeter大赛
- 德国：Chaos Communication Camp
- 荷兰：Hacking at Random
- 日本：信息安全知识技术竞赛
- 台湾：骇客年会HIT

Pwn2Own大赛/Pwnium大赛

- Pwn20wn：全球顶级黑客大赛之一，由安全研究机构TippingPoint DVLabs赞助。参赛黑客以四大浏览器（IE、Firefox、Chrome和Safari）为挑战目标。攻破一个主流浏览器便奖励1万美元，共4万美元，且参赛者不准使用Adobe Flash等第三方外挂。
- Pwnium：2011年起由谷歌主办的黑客大赛。2012年谷歌提供100万美元鼓励参赛者攻击Chrome浏览器，目的是帮助谷歌找到浏览器的缺陷，以便开发针对性的补丁。

Pwnium的来源

- Pwn20wn是以挑战四大浏览器为目的的黑客比赛，2007年至今已举办五届。
- 2009年谷歌公司Chrome浏览器首次参加Pwn20wn比赛，因参赛者大多已有破解的目标，所以并无黑客尝试破解Chrome浏览器，比赛中的安全漏洞及破解手法通常早在竞赛前就已经规划好。
- 2010-2011年谷歌在Pwn20wn比赛中额外提供2万美金鼓励黑客破解Chrome浏览器，但一直无人能够攻破Chrome。
- 2012年，Pwn2Own主办方规定不再要求获胜者公布漏洞发掘及利用过程，特别是沙箱环境的攻击过程，此举遭到谷歌反对，并导致谷歌撤出Pwn2Own 2012的资金赞助。Pwn2Own主办方称，如果漏洞发掘方法被公开，则没有黑客愿意再发掘Chrome浏览器漏洞。
- 2012年3月谷歌独自主办Pwnium大赛，并提供100万美金鼓励黑客攻击Chrome浏览器。2012年10月谷歌再次主办Pwnium大赛，并掷出200万美金奖励攻破Chrome浏览器的黑客。

Pwnium大赛奖金设置

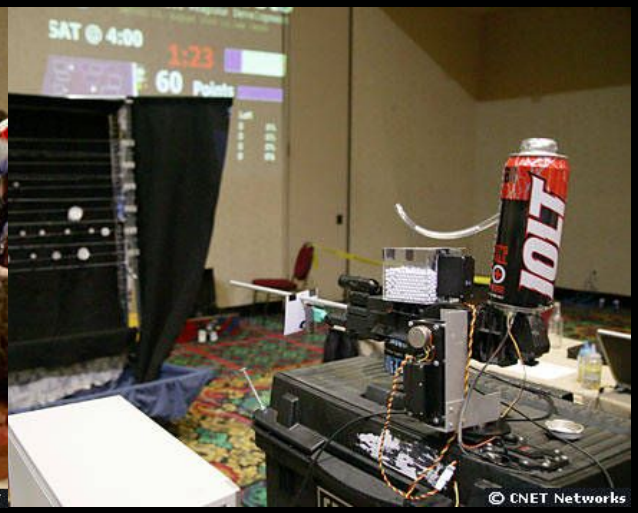
- 在比赛奖金的分配中，主要是针对Chrome浏览器的奖金。
- 对每一位能够入侵WindowsFlash或任一装置的驱动程序而让任何浏览器使用者产生安全问题的与赛者，Google公司也将给予2万美元奖金。
- 黑客若能找出与Chrome浏览器相关的弱点，有4万美元奖金。
- 找到Chrome浏览器的bug，则Google将加码至6万美元。

Black Hat大会

- 信息安全领域的顶级盛会，一个具有很强技术性的信息安全会议，会议引领安全思想和技术的走向，参会人员包括各个企业和政府的研究人员，甚至还有一些民间团队。为了保证会议能够着眼于实际并且能够最快最好地提出方案、问题的解决方法和操作技巧，会议环境保持中立和客观。

DEFCON黑客大会

- 以小规模讨论及技术切磋为主，会上流行的活动是若干人组成一个局域网，然后互相大打攻防战（CTF）。参赛者的目标是进攻对手的网络，但同时又得看好自己的地盘。由于想参加的队伍都得先经过会前淘汰赛，因此能入围最后大赛者都已经有相当实力。



Black Hat&DEFCON比较

- 由美国人杰夫•莫斯（现任美国安全顾问委员会顾问）分别于1992年和1997年创办，地点都在美国拉斯维加斯并且同期举行。
- Black Hat：比较正统和严谨，出席人员包括了世界各地的企业、政府、学术界及信息安全组织的思想领袖，议程表上包含各类专业人士的发言，内容则指向保障全球信息安全等主题。此外还会展示大量已被发现的数码产品安全漏洞，并演示骇客会如何进行攻击。
- DEFCON：与Black Hat风格正好相反，以小规模讨论为主，主题包括如何破解 Xbox，如何解锁苹果产品固件甚至如何入侵卫星系统，甚至讨论并试演各种被视为极具危险的技术元素。与会者可随意打扮，随意进出房间，或坐下来把腿架到桌子上听讲。

iCTF国际黑客竞赛

- 面向全球信息安全专业研究学生团队的大型在线黑客竞赛。
- iCTF’2011国际黑客竞赛的场景设计模拟目前黑帽子地下社区中的“洗钱产业链”，参赛队伍首先需要通过解决安全解谜挑战获得“黑钱”（Money），然后每支队伍需要通过分析挖掘出Gamebox中十个定制服务的安全漏洞，并攻陷其他对手所维护和防御的Gamebox来获得flag，取得flag之后还需要通过综合考虑每个服务的“洗钱佣金率”、“洗钱转换率”、“洗钱风险率”等“洗钱黑市行情”来计算优化的洗钱策略，逃避FBI追查并取得更好的洗钱效率，同时从“黑钱”到“白钱”的转化率也与每支队伍的Gamebox防御级别直接相关，此外竞赛还引入了队伍可以向FBI告发的机制用来破坏竞争对手的洗钱过程。

FACEBOOK黑客杯

- 黑客杯是Facebook组织的一场国际编程大赛，目的是帮助公司抢在谷歌等竞争对手之前，找到最聪明的年轻软件工程师。
- “黑客杯”大赛包括五轮挑战赛，即选拔赛、第一关比赛、第二关比赛、第三关比赛和决赛。
- 决赛后，第一名将奖励5000美元，获世界冠军称号，该荣誉镌刻在“黑客杯”奖品上。第二名将奖励2000美元，第三名奖励1000美元，第4-25名奖励100美元。第二关比赛中脱颖而出的前100名参赛者将获赠T恤。

POC安全大会

- Power of Community：由韩国黑客及安全专家发起的国际安全及黑客会议，以追求创新、交流、安全技术为名，崇尚知识分享，相信社区的力量可以使世界更安全。2012年POC安全大会的亮点在于由女孩们组成的CTF比赛。

2012年POC安全大会部分议题

- Andrei Costin：Ghost is in the Air(Traffic)
- Auriemma & Ferrante：Pwning Multiplayer Online Games
- flashsky：APT Attack Detection of Vulnhunt
- Gordeychik：SCADA Strange Love or How I Learned to Start Worrying and Love Nuclear Plants
- redhidden & silverbug：Fun of Firmware Hacking

Code Gate防黑客大赛

- 韩国知识经济部和韩国情报保护振兴院赞助。
- 比赛时长24小时，参赛者在比赛中必须解决密码破解、系统防御、病毒清除等各个方面的20个问题。
- 黑客在韩国的形象并不好，因此大赛制订了以'防御'为主的规则。
- 2008年Code Gate设置的总奖金为1亿韩元（约10万美元）
- 2009年Code Gate吸引了全世界41个国家的1750支黑客小组参加，冠军由韩国黑客队“Cpark”获得，并获得2000万韩元的冠军奖励。

PHDays CTF

- Positive Hack Days CTF是一个国际性信息安全竞赛，竞赛规则基于CTF，并贴近网络实战环境。竞赛分10-12只队伍，在规定时间内检测和修复己方环境漏洞并攻击其他队伍的网络环境。参赛队伍可以在竞赛中检验自己的实战能力，并开发自己的网络防护方案。

CodeMeter大赛

- 由德国威步公司主办，参赛者不仅免费得到保护应用程序，而且还可获得具有许可的CmStick硬件加密狗。1000多名来自世界各地的参赛者参与到了奖金总值为32768欧元（或美$ 40000）的比赛中。为了赢得比赛，每位参赛者必须要修改受CodeMeter保护的程序，已使它能够脱离CmDongle运行。
- 2007年比赛中包含两个模块的破解，程序只有在检测到CmDongle之后才能运行起来

  模块1: 该模块的许可已经包含在CmDongle中，可以直接运行

  模块2: 该模块的许可未被写入到CmDongle中

  两个模块的功能相同，都会显示一组密码

  任务：找出2个密码

  程序必须完全脱离CmDongle运行

  将破解方法和已破解程序通过Email发送至威步公司

Chaos Communication Camp

- 也被称为“欧洲黑客大会”，由德国Chaos Computer Club（CCC）主办的为期五天的露天黑客交流活动，每五年举办一次。
- 会议以技术及社会话题为主，包括隐私、信息自由、数据安全等等。
- 每位参与者都可带一顶帐篷加入营地活动，营地准备有电源、网络及食物等等。



Hacking at Random

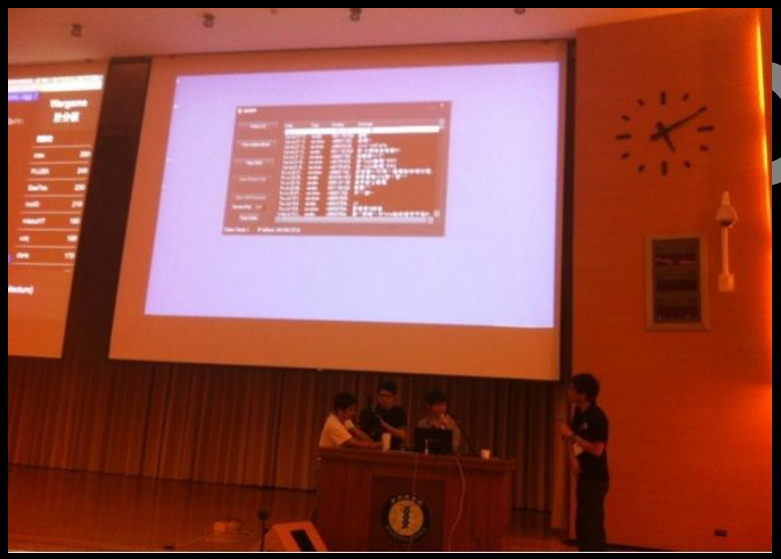
- 在荷兰博克斯特尔举办的室外黑客夏令营，也是欧洲最大的黑客夏令营。
- 该聚会始于1989年的银河黑客聚会，之后该会议每四年举办一次，每次主题均不同：2005年为“What The Hack”、2009年为“Hacking at Random”、2013年为“Observe. Hack. Make.”
- 会议主题不一而足，例如讨论互联网警察的最新技术，欧洲软件专利法可能带来的后果，如何自我保护个人数据，发展中国家的无线上网机会等等。

日本信息安全知识技术竞赛

- 以模拟网络战的形式，让参赛者通过黑客技术侵入敌方网络，或者抵御对方的攻击。
- 各地竞赛采用提问形式，要求选手以网 络攻防所必需的知识作答。选手们必须在规定的10个小时之内挑战并完成有关密码、程序和网络等方面的50个问题。最后由各地的优胜者以对战形式参加全国总决赛。

台湾骇客年会HIT

- Hacks In Taiwan (HIT) 台湾骇客年会是台湾最大的骇客与安全技术研讨会。除了面对面技术交流外，会议期间还有网络攻防赛（Wargame），提供真实的网络环境和挑战，以及IRC聊天室和绵羊墙。



2012年台湾骇客年会部分议题

- Pedro.Vilaca：Past and Future in OX X Malware
- Aido&Manaka：Emergency.Headquarters.Basara
- Kouni.Miyamoto：VMdetection.Maniacs
- CHROOT.PK：Pwning.Chinese.P2P.Network
- Andrey.Belenko：Evolution.of.iOS.Data.Protection
- CHROOT.Dark：iOS.Game.Reversing
- PCCU.Chou：Cryptanalysis in real life.V2

国外其他黑客大赛

- 希腊：AthC0n
- 美国：GrrCon
- 加拿大：Hackfest
- 拉丁美洲：H2HC
- 美国：SkyDogCon
- 美国：THOTCON

AthC0n

- 欧洲东南部最大的黑客会议，每年在希腊雅典举办。
- 2013年举办第一届CTF比赛，并由赛门铁克赞助，有超过15名参赛者参加。

GrrCon

- 每年九月份在美国密歇根州大急流城举办，并聚集首席安全官、安全研究人员、安全爱好者、黑客的会议。
- 该会议黑客比赛及活动包括CTF比赛、取证挑战赛、开锁大赛、多种工作坊等等。

Hackfest

- 在加大那魁北克举办的集黑客会议和黑客比赛于一体的活动。
- 2014年Hackfest的黑客竞赛为16小时制，比赛被命名为“King of Hill”，目标包括控制目标服务器和防护目标服务器。
- 为纪念比特币，2014年的Hackfest活动另有中本聪和莱恩.富格尔在现场举办“reversing de cryptomonaie”挑战赛。

H2HC

- H2HC是拉丁美洲最有年头的安全会议，也是世界上举办年头最多且依然活跃的黑客会议之一。

SkyDogCon

- 美国纳什维尔市的技术会议，旨在以文艺复兴思想促进学习、交流、分享和不同领域技术人员的融合。
- SkyDogCon的竞赛包括：
  CTF比赛
  社会工程CTF比赛
  危险！黑客
  电子徽章挑战赛
  加密解密挑战赛
  照片竞赛
  开锁竞赛
  乐高积木挑战赛
  微缩世界挑战赛




THOTCON

- 每年春天在美国芝加哥举办的黑客会议，是芝加哥非官方、非盈利的活动。2014年的THOTCON黑客竞赛方式与技术完全无关，两种竞赛方式分别是T恤设计竞赛和黑客酿酒竞赛。
- T恤设计竞赛：提交T恤设计方案，设计最优者将获得VIP门票。
- 黑客酿酒竞赛：每名黑客提交自己酿造的啤酒参与评判，获胜者将获得一些奖励。参赛者仅可自带一瓶啤酒参赛且必须为THOTCON参会人员。

中外黑客比赛对比

	国内信息安全竞赛	国外/地区黑客比赛
竞赛背景	主要由官方主办	由民间组织/企业主办
竞赛目的	选拔、培训人才	增进技术交流、信息共享
竞赛内容	传统信息安全	不限技术领域的信息安全话题/主题
竞赛方式	理论答题+信息攻防比赛	不限技术领域的技术切磋、交流、探讨及网络攻防实战
技术领域	针对性弱，覆盖面广	针对性强，技术新颖
奖项设置	证书奖励为主，现金奖励为辅	现金奖励为主

国内CTF及IDF实验室发展

- 国内CTF与国外CTF差距？
- 国内CTF的定位与发展？

- IDF的定位？
- IDF的发展？
- IDF成员构成？
- IDF活动组织？

谢谢!