BlackHat USA 2014 参会纪实

世界著名的网络安全黑客会议黑帽子(BlackHat)大会于北美当地时间 2014 年 8 月 6 日开幕了。世界著名的网络安全黑客会议黑帽子(BlackHat)大会于北美当地时间 2014 年 8 月 6 日开幕了。

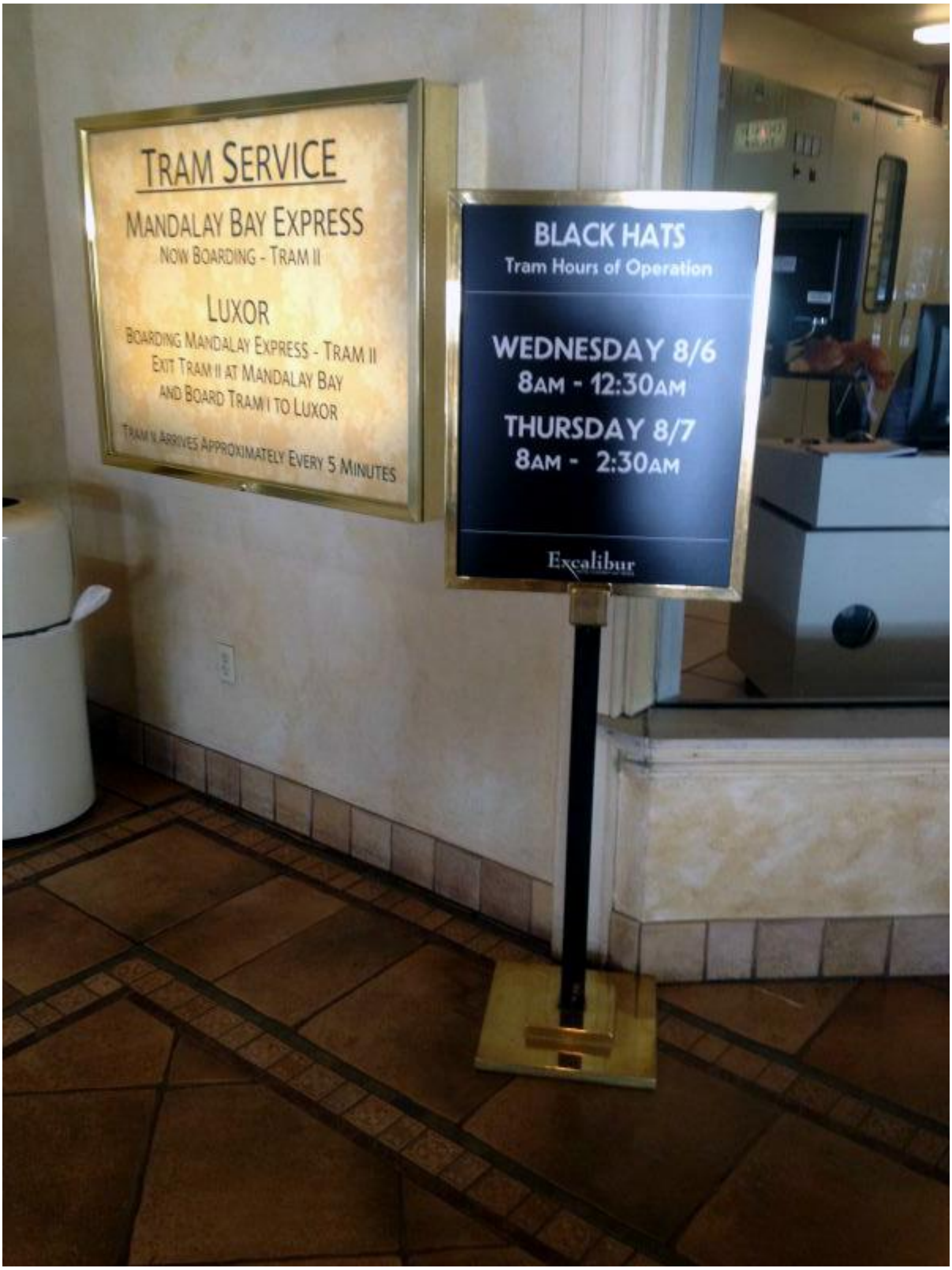
而习科现任的开发主管与一名小编有幸从中国来到了美国 XX 之都拉斯维加斯(Las Vegas)参加黑帽大会。

首先小编要纠正一些媒体的报道，虽然黑帽官网公布的时间是 8 月 2 号到 7 号，但是 5 号之前的 4 天是安全培训课程，培训课程从每门$2000 到$5000 不等。真正有看点的安全研究报告会议的开幕是从 6 号开始的，共分 9 个会场，小编也只能选取最感兴趣的几场参加。

因为往期有不少中国安全厂商、媒体参加，所以小编以前参加黑帽大会的情况并没有给大家分享。

今年因为 XXX 的原因，美国通过拒发签证来阻止中国黑客和安全厂商参加黑帽大会，而且会场又禁止摄像，所以小编这次给大家分享一下参会的经过吧。

在乘轻轨的地方就看到黑帽主办方的指引牌子。



指引牌上面的会议时间着实雷到小编了，第一天的 party 到次日凌晨半点，第二天的 party 到次日凌晨两点半。这个 party 着实有点狠。

一路上同行乘轻轨的人一眼看过去就知道是不是来参加黑帽的，例如小编前面的两个疑似印度人的黑阔哥哥。

从这个通道过来，就已经属于黑阔专属领地了，小编看看窗外的景色，心中暗骂一句：沙漠绿洲小城市，这万恶的资本主义呀！

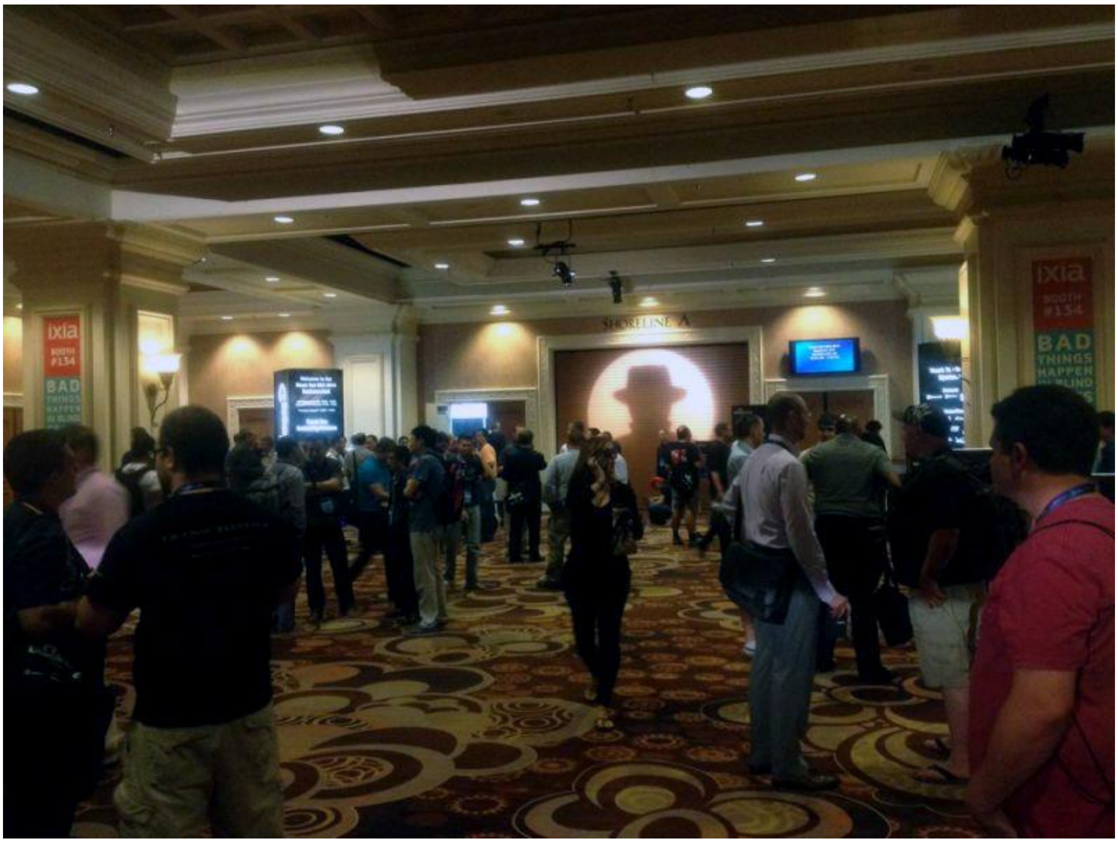
进到会场以后发现来自世界各地的大黑阔们有很多都穿着自己的黑阔战队的队服，当然了，绝大部分参会者比较成熟稳重事业型，像国内的小黑类型的人基本见不到。

来到登记处发现登记设备略 diao，全都是自助式操作，不知道这些计算机有没黑阔日进去挂马搞个键盘记录什么的。

{说起来小编之前设置了手机收发 Email，登录了一次黑帽官方提供的无线以后，刚刚发现小编的邮箱已经有多次异常登录的提醒了。

开幕致辞结束以后，这些黑客们三三两两的就开始坐在一起搞黑帽官方提供的无线网络，各种设备各种系统，各种工具各种神器，各种扫各种日，永远都是惊奇。

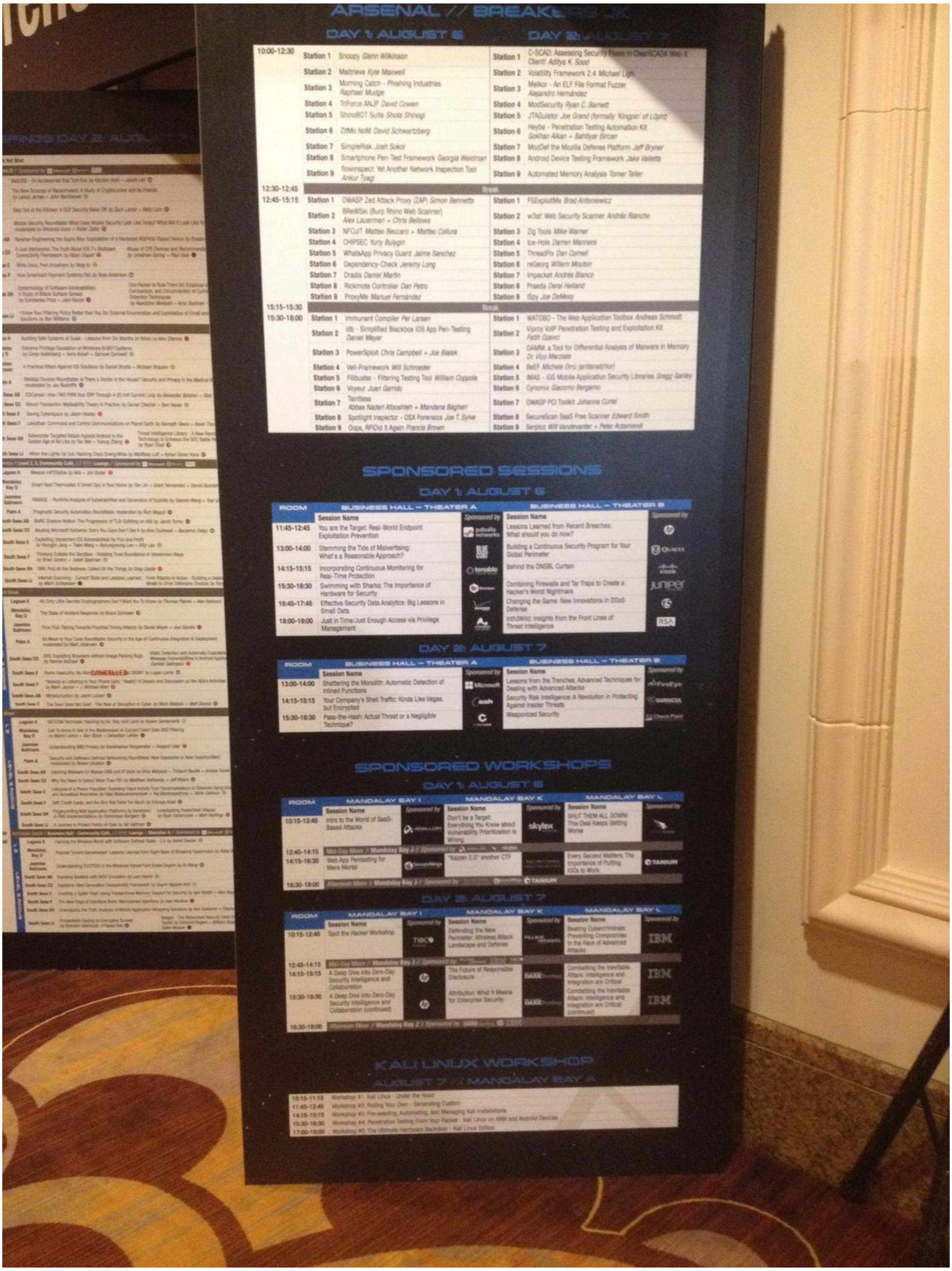
赞助商的展览厅中不时有 Show Girl 走出来玩，完全不搭理的节奏：“尼玛这附近开房 300 到 500 刀，还不如老子日无线痛快”，穷屌注定孤独一生。



在会场外偶遇一只间谍妹子，问小编我是怎么知道的？带墨镜，一身黑衣服，打电话还不时环顾四周，有事业线又不做 Show Girl，无论是参会黑客，演讲者还是赞助商，出入会场都需要佩戴有效名称的证件，这只妹子证件不带名字哦。

小编不懂英语，但是 25 个字母全认识啊有木有！！！最关键的就是这枚妹子在电话中提到了 C~I~A~

到处都在搞无线，这枚红帽妹子长发及腰，胸大腿长，目测这两个人是不同的黑客战队间在“切磋武艺”



ARSENAL // BREAKE[illegible]K

	DAY 1: AUGUST 6		DAY 2: AUGUST 7	
10:00-12:30	Station 1	Snoopy *Glenn Wilkinson*	Station 1	C-SCAD: Assessing Security Flaws in ClearSCADA Web-X Client! *Aditya K. Sood*
	Station 2	Maltrieve *Kyle Maxwell*	Station 2	Volatility Framework 2.4 *Michael Ligh*
	Station 3	Morning Catch - Phishing Industries *Raphael Mudge*	Station 3	Melkor - An ELF File Format Fuzzer *Alejandro Hernández*
	Station 4	TriForce ANJP *David Cowen*	Station 4	ModSecurity *Ryan C. Barnett*
	Station 5	ShinoBOT Suite *Shota Shinogi*	Station 5	JTAGulator *Joe Grand (formally 'Kingpin' of L0pht)*
	Station 6	ZitMo NoM *David Schwartzberg*	Station 6	Heybe - Penetration Testing Automation Kit *Gokhan Alkan + Bahtiyar Bircan*
	Station 7	SimpleRisk *Josh Sokol*	Station 7	MozDef the Mozilla Defense Platform *Jeff Bryner*
	Station 8	Smartphone Pen-Test Framework *Georgia Weidman*	Station 8	Android Device Testing Framework *Jake Valletta*
	Station 9	flowinspect: Yet Another Network Inspection Tool *Ankur Tyagi*	Station 9	Automated Memory Analysis *Tomer Teller*
12:30-12:45	Break			
12:45-15:15	Station 1	OWASP Zed Attack Proxy (ZAP) *Simon Bennetts*	Station 1	FSExploitMe *Brad Antoniewicz*
	Station 2	BReWSki (Burp Rhino Web Scanner) *Alex Lauerman + Chris Bellows*	Station 2	w3af: Web Security Scanner *Andrés Riancho*
	Station 3	NFCulT *Matteo Beccaro + Matteo Collura*	Station 3	Zig Tools *Mike Warner*
	Station 4	CHIPSEC *Yuriy Bulygin*	Station 4	Ice-Hole *Darren Manners*
	Station 5	WhatsApp Privacy Guard *Jaime Sanchez*	Station 5	ThreadFix *Dan Cornell*
	Station 6	Dependency-Check *Jeremy Long*	Station 6	reGeorg *Willem Mouton*
	Station 7	Dradis *Daniel Martin*	Station 7	Impacket *Andrés Blanco*
	Station 8	Rickmote Controller *Dan Petro*	Station 8	Praeda *Deral Heiland*
	Station 9	ProxyMe *Manuel Fernández*	Station 9	iSpy *Joe DeMesy*
15:15-15:30	Break			
15:30-18:00	Station 1	Immunant Compiler *Per Larsen*	Station 1	WATOBO - The Web Application Toolbox *Andreas Schmidt*
	Station 2	idb - Simplified Blackbox iOS App Pen-Testing *Daniel Mayer*	Station 2	Viproy VoIP Penetration Testing and Exploitation Kit *Fatih Ozavci*
	Station 3	PowerSploit *Chris Campbell + Joe Bialek*	Station 3	DAMM: a Tool for Differential Analysis of Malware in Memory *Dr. Vico Marziale*
	Station 4	Veil-Framework *Will Schroeder*	Station 4	BeEF *Michele Orrù (antisnatchor)*
	Station 5	Filibuster - Filtering Testing Tool *William Coppola*	Station 5	iMAS - iOS Mobile Application Security Libraries *Gregg Ganley*
	Station 6	Voyeur *Juan Garrido*	Station 6	Cynomix *Giacomo Bergamo*
	Station 7	Taintless *Abbas Naderi Afooshteh + Mandana Bagheri*	Station 7	OWASP PCI Toolkit *Johanna Curiel*
	Station 8	Spotlight Inspector - OSX Forensics *Joe T. Sylve*	Station 8	SecureScan SaaS Free Scanner *Edward Smith*
	Station 9	Oops, RFIDid It Again *Francis Brown*	Station 9	Serpico *Will Vandevanter + Peter Arzamendi*

SPONSORED SESSIONS

DAY 1: AUGUST 6

ROOM	BUSINESS HALL – THEATER A		BUSINESS HALL – THEATER B	
	Session Name	Sponsored by	Session Name	Sponsored by
11:45-12:45	You are the Target: Real-World Endpoint Exploitation Prevention	paloalto networks	Lessons Learned from Recent Breaches: What should you do now?	hp
13:00-14:00	Stemming the Tide of Malvertising: What's a Reasonable Approach?	BLUE COAT	Building a Continuous Security Program for Your Global Perimeter	QUALYS
14:15-15:15	Incorporating Continuous Monitoring for Real-Time Protection	tenable	Behind the DNSBL Curtain	cisco
15:30-16:30	Swimming with Sharks: The Importance of Hardware for Security	Bromium	Combining Firewalls and Tar Traps to Create a Hacker's Worst Nightmare	juniper
16:45-17:45	Effective Security Data Analytics: Big Lessons in Small Data	[illegible]	Changing the Game: New Innovations in DDoS Defense	f5
18:00-19:00	Just in Time/Just Enough Access via Privilege Management	[illegible]	Inth3Wild: Insights from the Front Lines of Threat Intelligence	RSA

DAY 2: AUGUST 7

ROOM	BUSINESS HALL – THEATER A		BUSINESS HALL – THEATER B	
	Session Name	Sponsored by	Session Name	Sponsored by
13:00-14:00	Shattering the Monolith: Automatic Detection of Inlined Functions	Microsoft	Lessons from the Trenches: Advanced Techniques for Dealing with Advanced Attacks	FireEye
14:15-15:15	Your Company's Shell Traffic: Kinda Like Vegas, but Encrypted	ssh	Security Risk Intelligence: A Revolution in Protecting Against Insider Threats	GURUCUL
15:30-16:30	Pass-the-Hash: Actual Threat or a Negligible Technique?	C	Weaponized Security	Check Point

SPONSORED WORKSHOPS

DAY 1: AUGUST 6

ROOM	MANDALAY BAY I		MANDALAY BAY K		MANDALAY BAY L	
	Session Name	Sponsored by	Session Name	Sponsored by	Session Name	Sponsored by
10:15-12:45	Intro to the World of SaaS-Based Attacks	ADALLOM	Don't be a Target: Everything You Know about Vulnerability Prioritization is Wrong	skybox	SHUT THEM ALL DOWN! This Deal Keeps Getting Worse	[illegible]
12:45-14:15	Mid-Day Mixer // Mandalay Bay J // Sponsored by: [illegible]					
14:15-16:30	Web App Pentesting for Mere Mortal	[illegible]	"Kaizen 2.0" another CTF	[illegible]	Every Second Matters: The Importance of Putting IOCs to Work	TANIUM
16:30-18:00	Afternoon Mixer // Mandalay Bay J // Sponsored by: [illegible] TANIUM					

DAY 2: AUGUST 7

ROOM	MANDALAY BAY I		MANDALAY BAY K		MANDALAY BAY L	
	Session Name	Sponsored by	Session Name	Sponsored by	Session Name	Sponsored by
10:15-12:45	Spot the Hacker Workshop	TIBCO	Defending the New Perimeter: Wireless Attack Landscape and Defense	FLUKE networks	Beating Cybercriminals: Preventing Compromise in the Face of Advanced Attacks	IBM
12:45-14:15	Mid-Day Mixer // Mandalay Bay J // Sponsored by: [illegible]					
14:15-15:15	A Deep Dive into Zero-Day Security Intelligence and Collaboration	hp	The Future of Responsible Disclosure	DARK Reading	Combatting the Inevitable Attack: Intelligence and Integration are Critical	IBM
15:30-16:30	A Deep Dive into Zero-Day Security Intelligence and Collaboration (continued)	hp	Attribution: What It Means for Enterprise Security	DARK Reading	Combatting the Inevitable Attack: Intelligence and Integration are Critical (continued)	IBM
16:30-18:00	Afternoon Mixer // Mandalay Bay J // Sponsored by: DARK Reading hp IBM					

KALI LINUX WORKSHOP

AUGUST 7 // MANDALAY BAY A

10:15-11:15	Workshop #1: Kali Linux - Under the Hood
11:45-12:45	Workshop #2: Rolling Your Own - Generating Custom
14:15-15:15	Workshop #3: Pre-seeding, Automating, and Managing Kali Installations
15:30-16:30	Workshop #4: Penetration Testing From Your Pocket - Kali Linux on ARM and Android Devices
17:00-18:00	Workshop #5: The Ultimate Hardware Backdoor - Kali Linux Edition

看人的同时小编抽空看了下会议日程的安排，目测共 9 个会场具体议程都在上面拉，目测场场无尿点，小编分身乏力，只期盼 Defcon 能好一些。

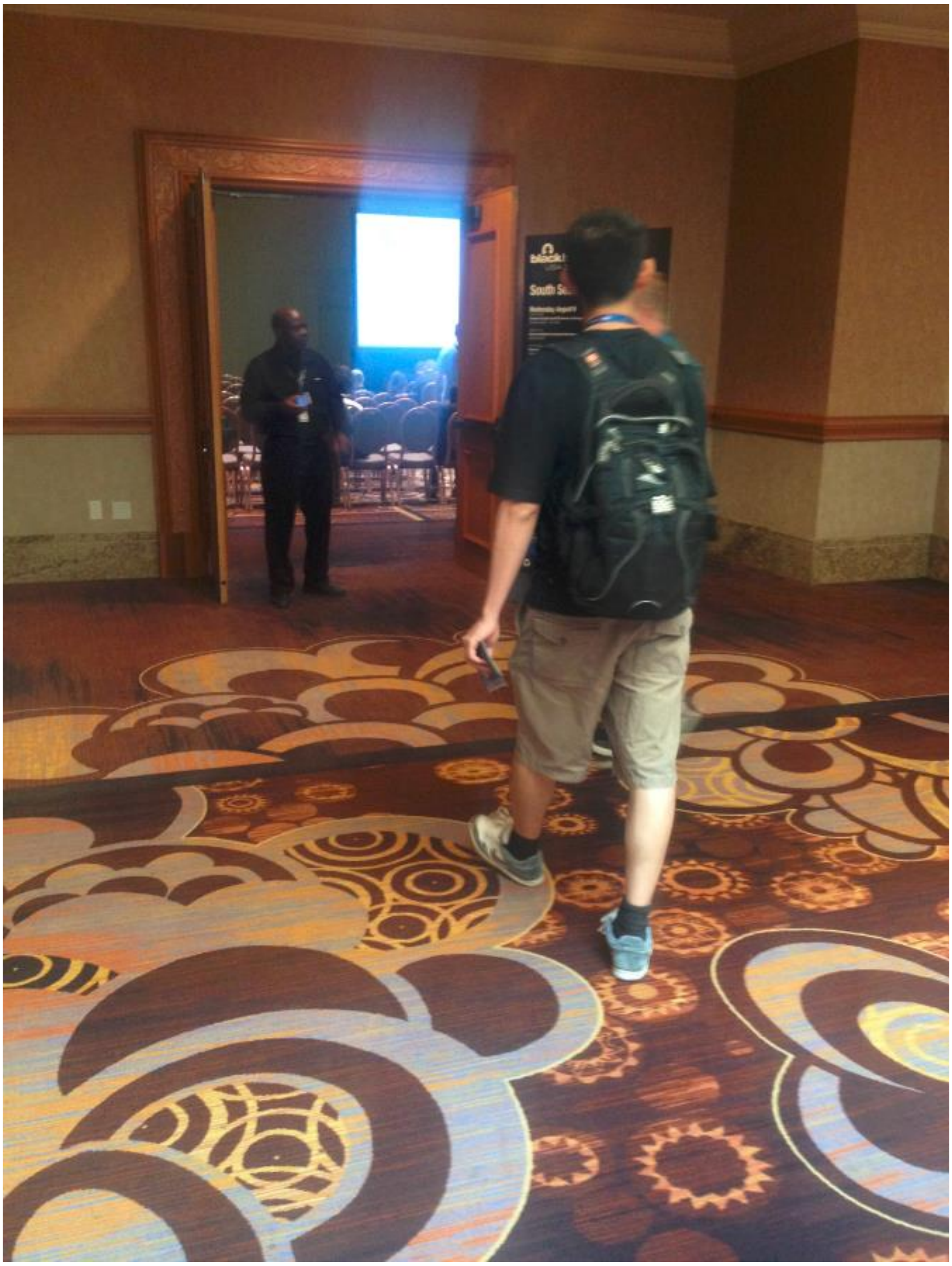
如果要说黑帽大会的尿点，应该就是当会议要开始的时候了吧，在相机拍不到的地方至少还有能见到的这些人的三倍数量。

照片中有一支黑客战队很显眼，猜猜他们是哪一支？很有名哦。

小编只想说，黑阔这么多，酒店真的没被脱库吗？

小编只想说，黑阔这么多，酒店真的没被脱库吗？

趁人山人海之前主管大人走就偷偷的入场了。



至于演讲，按尿性通常演讲者研究的很深入，但是他们讲的东西通常很浅，思路很好，其他纯属装逼，今年也不例外。例如一个哥们的演讲说自己怎样怎样搞起来一套东西，自动注册亚马逊等云主机，自动注册邮箱以及自动通过 Email 验证等.。

然后拿获得的机器去挖矿。一天不济也能挖个二三百，注意是刀，刀乐美元。

可是呢，我们要的是东西是干货，您光说您自己逼格是够高了，可是我们的门票钱还没捞回来哪！万恶的资本主义呀，俺靠！

Targeted Cyber Attacks
Network and System Security
Social Media Security
Social Engineering Penetration Test
Unified Communications Forensics
Cloud Storage Forensics
Metasploit
The Penetration Tester's Guide
Metasploit
The Penetration Tester's Guide
HACKING
Managing Information Security Breaches
Practical Reverse Engineering
Social Engineering
Database Hacker's Handbook
Delegate Bag

于是小编奋而离席，还是原版书籍比较吸引人，虽然贵了点，拿回去也能小小的装一把不是。

至于最后赠品嘛，什么 ipad，外星人之类的通通没有咱们的份，送了一包心脏出血的小糖果倒是挺不错。

其他的像星巴克 5 块钱抵用券，诺顿手机防护，小东西也不少。至于这个正宗 Made in USA 的黑帽限量款 ZIPPO 打火机，小编们不抽烟，哪位烟民想。。。？

会议结束后，小编没有参加黑帽的 party。

同样是来的时候的通道，进去的时候是 Welcome，走的时候仍然是 Welcome，只不过走的时候欢迎横幅是欢迎参加明年的会议了。

到了公交车站以后，公交车售票机疑似被某黑客战队按进去几千个钢板，愣是把硬币计数器按到溢出正无穷，再退币后把机器所有硬币都给吐了出来，现在售票机罢工啦。

于是小编一行四个人步行走了两个小时，找了个中文服务的 ATM 取款机才放心的取款。

最后，这就是黑帽大会啦，没有想象中的那么无所不能，却总是无时无刻不给我们带来惊喜。