出國報告（出國類別：其他國際會議）

出席「國際資訊安全會議(DEF CON 23)」報告

服務機關：行政院資通安全辦公室
姓名職稱：周智禾 諮議
派赴國家：美國(拉斯維加斯)
出國期間：104 年 8 月 5 日至 104 年 8 月 11 日
報告日期：104 年 10 月 19 日

摘　　要

近年來，網路攻擊事件頻傳，資訊安全問題已成為國際關注之重要議題，各國亦定期召開資安相關會議以交流最新資安發展趨勢，包含 Blackhat、DEF CON 及 RSA Conference 等。其中， DEF CON 係全球最盛大的資訊安全會議，每年均於美國拉斯維加斯舉辦，內容包含豐富的資安趨勢論壇及最新的資安軟硬體設備展覽，已成為國際間年度最重要的資訊安全會議之一。

本(104)年 DEF CON(第 23 次)於拉斯維加斯 Paris 和 Bally’s 會議中心舉辦為期 4 日會議(8 月 6 至 9 日)，內容包含多場次的資安技術研討會，以及國際間最重要的網路攻防競賽(Capture the Flag, CTF)。透過前開會議，我們可以觀察到近來堀起的資安技術及標準、最新的駭客研究，會議中亦發表許多被揭露出的安全議題，包括雲端、行動裝置、網頁技術及滲透測試相關議題等。本次會議主題除了傳統的網站應用安全議題外，車載(Vehicle)系統安全性及行動裝置駭侵技術的議題亦在此次的會議中受到相當程度的重視。

目　　錄

壹、會議介紹

一、會議名稱

DEF CON 23(第 23 屆戰備大會)

二、會議時間

2015 年 8 月 6 至 2015 年 8 月 9 日

三、會議地點

美國拉斯維加斯 Paris 和 Bally’s 會議中心

四、會議相關文件

會議相關資料請詳見網站(https://www.defcon.org/html/defcon-23/dc-23-index.html)

貳、參加會議目的

DEF CON 為目前世界上最盛大的駭客會議，迄今已舉辦 23 屆，每年超過 1 萬名的駭客，以及資(安)訊界、廠商、政府機關、學研界等資安專業人員齊聚於美國拉斯維加斯，旨在交流資安最新趨勢、攻防最新手法及系統最新弱點。DEF CON 會議門票係採不記名方式僅能透過現場排隊購買(等待時間平均至少 3 小時以上)，因此，主辦單位亦沒有與會者名單，讓該會議始終保持著神秘色彩。

會議主要可分為演講、駭客村(Villages)、CTF、Workshop 等部分，本次出國主要目的係參加各場次的演講，並參觀不同主題的駭客村(Crypto & Privacy Village、Hardware Hacking Village、Lockpick Village、Packet Hacking Village、Tamper Evident Village、Wireless Village、Car Hacking Village、Bio Hacking Village、Social Engineering Village、Data Village、ICS Village、Internet of Things Village)；此外，該會議備受矚目的 CTF 競賽係由世界各國頂尖駭客團隊所進行的網路攻防競賽，我國 HITCON 團隊於去(103)年首度進入決賽即取得第 2 名佳績，本年 CTF 競賽由包含我國 HITCON 團隊在內的 15 個參賽隊伍角逐冠軍。

參、會議過程及重點議題

一、會議議程

DEF CON 23 演講議程自 8 月 6 日(四)至 8 月 9 日(日)，共分為 5 個廳進行演講，包括「Track One」、「Track Two」、「Track Three」、「Track Four」及「Defcon 101」，議程詳如表 1 至表 4：

表 1：DEF CON 23 會議第 1 日議程(8 月 6 日)

Time	TRACK FOUR	DEF CON 101
10:00	Hardware and Trust Security: Explain it like I'm 5 Teddy Reed & Nick Anderson	Introduction to SDR and the Wireless Village DaKahuna & satanklawz
11:00	Hacking Web Apps Brent White	Hackers Hiring Hackers - How to Do Things Better Tottenkoph & IrishMASMS
12:00	Seeing through the Fog Zack Fasel	DEF CON 101: The Panel Panel
13:00	Alice and Bob are Really Confused David Huerta	
14:00	Hacker in the Wires Dr. Phil Polstra	Beyond the Scan: The Value Proposition of Vulnerability Assessment Damon Small
15:00	Forensic Artifacts From a Pass the Hash Attack Gerard Laygui	Responsible Incident: Covert Keys Against Subverted Technology Latencies, Especially Yubikey 1o57
16:00	Sorry, Wrong Number: Mysteries Of The Phone System — Past and Present "Unregistered436" & "Snide" Owen	Guests N' Goblins: Exposing Wi-Fi Exfiltration Risks and Mitigation techniques Peter Desfigies, Joshua Brierton & Naveed Ul Islam
17:00	Backdooring Git John Menerick	Dark side of the ELF — leveraging dynamic loading to pwn noobs Alessandro Di Federico & Yan

		Shoshitaishvil
18:00	Secure Messaging for Normal People Justin Engler	Medical Devices: Pwnage and Honeypots Scott Erven & Mark Collao

表 2：DEF CON 23 會議第 2 日議程(8 月 7 日)

Time	TRACK ONE	TRACK TWO	TRACK THREE	TRACK FOUR	DEF CON 101
10:00	Shall We Play a Game? Tamas Szakaly	Working together to keep the Internet safe and secure Alejandro Mayorkas	Welcome to DEF CON DT and 1057	Bugged Files: Is Your Document Telling on You? Daniel "unicornFurnace" Crowley & Damon Smith	NSM 101 for ICS Chris Sistrunk
11:00	Stagefright: Scary Code in the Heart of Android Joshua J. Drake	Licensed to Pwn: The Weaponization and Regulation of Security Research Panel	Fighting Back in the War on General Purpose Computers Cory Doctorow	Goodbye Memory Scraping Malware: Hold Out Till "Chip And Pin" Weston Hecker	Crypto for Hackers Eijah
12:00	Malware in the Gaming Micro-economy Zack Allen & Rusty Bower	Licensed to Pwn: The Weaponization and Regulation of Security Research cont.	USB Attack to Decrypt Wi-Fi Communications Jeremy Dorrough	Confessions of a Professional Cyber Stalker Ken Westin	Bruce Schneier Q&A Bruce Schneier
13:00	Insteon' False Security And Deceptive Documentation Peter Shipley & Ryan Gooler	Drive It Like You Hacked It: New Attacks and Tools to Wirelessly Steal Cars Samy Kamkar	Red vs. Blue: Modern Active Directory Attacks & Defense Sean Metcalf	Don't Whisper my Chips: Sidechannel and Glitching for Fun and Profit Colin O'Flynn	Applied Intelligence: Using Information That's Not There Michael Schrenk
14:00	Build a free cellular traffic capture tool with a vxworks based femoto Yuwei Zheng &	How to Hack a Tesla Model S Marc Rogers & Kevin Mahaffey	Remote Access, the APT Ian Latter	Cracking Cryptocurrency Brainwallets Ryan Castellucci	Hacking SQL Injection for Remote Code Execution on a LAMP stack Nemus

	Haoqi Shan				
15:00	How to hack your way out of home detention AmmonRa	Low-cost GPS simulator - GPS spoofing by SDR Lin Huang & Qing Yang	REvisiting RE:DoS Eric (XlogicX) Davisson	Quantum Computers vs. Computers Security Jean-Philippe Aumasson	Chellam - a Wi-Fi IDS/Firewall for Windows Vivek Ramachandran
16:00	HamSammich - long distance proxying over radio Robert Graham & David Maynor	Harness: Powershell Weaponization Made Easy (or at least easier) Rich Kelley	When the Secretary of State says: "Please Stop Hacking Us…" David An	Tell me who you are and I will tell you your lock pattern Marte Løge	LTE Recon and Tracking with RTLSDR Ian Kline
16:30	How to secure the keyboard chain Paul Amicelli & Baptiste David	I Will Kill You Chris Rock	Put on your tinfo_t hat if you're my type miaubiz	Separating Bots from the Humans Ryan Mitchell	Detecting Randomly Generated Strings; A Language Based Approach Mahdi Namazifar
17:00	When IoT attacks: hacking a Linux-powered rifle Runa A. Sandvik & Michael Auger	Fun with Symboliks atlas	NetRipper - Smart traffic sniffing for penetration testers Ionut Popescu	Hack the Legacy! IBM i (aka AS/400) Revealed Bart Kulach	I Am Packer And So Can You Mike Sconzo
18:00	How to Train Your RFID Hacking Tools Craig Young	Drinking from LETHE: New methods of exploiting and mitigating memory corruption vulnerabilities Daniel Selifonov	Hooked Browser Meshed-Networks with WebRTC and BeEF Christian (@xntrik) Frichot	Breaking SSL Using Time Synchronisation Attacks Jose Selvi	Rocking the Pocket Book: Hacking Chemical Plant for Competition and Extortion Marina Krotofil & Jason Larsen
19:00	One Device to Pwn Them All Dr. Phil				

	Polstra				

表 3：DEF CON 23 會議第 3 日議程(8 月 8 日)

Time	TRACK ONE	TRACK TWO	TRACK THREE	TRACK FOUR	DEF CON 101
10:00	Scared Poopless - LTE and *your* laptop Mickey Shkatov & Jesse Michael	ThunderStrike 2: Sith Strike Trammel Hudson, Xeno Kovah, Corey Kallenberg	Do Export Controls on "Intrusion Software" Threaten Vulnerability Research? Tom Cross aka Decius & Collin Anderson	Dissecting the Design of SCADA Web Human Machine Interfaces (HMIs) - Hunting Vulnerabilities Aditya K Sood	A Hacker's Guide to Risk Bruce Potter
11:00	Key-Logger, Video, Mouse — How To Turn Your KVM Into a Raging Key-logging Yaniv Balmas & Lior Oppenheim	Machine vs. Machine: Inside DARPA's Fully Automated CTF Michael Walker & Jordan Wiens	'DLL Hijacking' on OS X? #@%& Yeah! Patrick Wardle	QARK: Android App Exploit and SCA Tool Tony Trummer & Tushar Dalvi	And That's How I Lost My Other Eye: Further Explorations In Data Destruction Zoz
12:00	Hacking Smart Safes: On the "Brink" of a Robbery Dan "AltF4" Petro & Oscar Salazar	F*ck the attribution, show us your .idb! Morgan Marquis-Boire, Marion Marschalek, Claudio Guarnieri	I Hunt Penetration Testers: More Weaknesses in Tools and Procedures Wesley McGrew	Chigula — a framework for Wi-Fi Intrusion Detection and Forensics Vivek Ramachandran	Are We Really Safe? - Bypassing Access Control Systems Dennis Maldonado
13:00	Spread Spectrum Satcom Hacking: Attacking The GlobalStar Simplex Data Service Colby Moore	Angry Hacking - the next generation of binary analysis Yan Shoshitaishvili & Fish Wang	WhyMI so Sexy? WMI Attacks, Real-Time Defense, and Advanced Forensic Analysis Matt Graeber, Willi Ballentin,	From 0 To Secure In 1 Minute — Securing IAAS Nir Valtman & Moshe Ferber	It's The Only Way To Be Sure: Obtaining and Detecting Domain Persistence Grant Bugher

			Claudiu Teodorescu		
14:00	Extracting the Painful (blue)tooth Matteo Beccaro & Matteo Collura	Remote exploitation of an unaltered passenger vehicle Charlie Miller and Chris Valasek	WhyMI so Sexy? WMI Attacks, Real-Time Defense, and Advanced Forensic Analysis cont.	BurpKit — Using WebKit to Own the Web Nadeem Douba	Abusing XSLT for Practical Attacks Fernando Arnaboldi
15:00	Looping Surveillance Cameras through Live Editing of Network Streams Eric Van Albert & Zach Banks	Hacking Electric Skateboards: Vehicle Research For Mortals Mike Ryan & Richo Healey	High-Def Fuzzing: Exploring Vulnerabilities in HDMI-CEC Joshua Smith	Let's Encrypt - Minting Free Certificates to Encrypt the Entire Web Peter Eckersley, James Kasten, & Yan Zhu	Extending Fuzzing Grammars to Exploit Unexplored Code Paths in Modern Web Browsers Saif El-Sherei & Etienne Stalmans
16:00	Switches Get Stitches Colin Cassidy, Éireann Leverett, Robert M. Lee	I want these * bugs off my * Internet Dan Kaminsky	Investigating the Practicality and Cost of Abusing Memory Errors with DNS Luke Young	NSA Playset: JTAG Implants Joe FitzPatrick & Matt King	How to Shot Web: Web and mobile hacking in 2015 Jason Haddix
17:00	Exploring Layer 2 Network Security in Virtualized Environments Ronny L. Bull & Jeanna N. Matthews	Security Necromancy: Further Adventures in Mainframe Hacking Philip Young & Chad "Bigendian Smalls" Rikansrud	802.11 Massive Monitoring Andres Blanco & Andres Gazzoli	Hacking the Human Body/brain: Identity Shift, the Shape of a New Self, and Humanity 2.0 Richard Thieme	The Bieber Project: Ad Tech 101, Fake Fans and Adventures in Buying Internet Traffic Mark Ryan Talabis
18:00	Staying Persistent in Software Defined Networks	Ask the EFF: The Year in Digital Civil Liberties Panel	DEF CON Comedy Inception: How many levels deep can we go? Panel	DIY Nukeproofing: a new dig at "data-mining" 3AlarmLampscooter	Game of Hacks: Play, Hack & Track Amit Ashbel & Maty Siman

	Gregory Pickett				
19:00	Contest: Drunk Hacker History Until 20:20	Ask the EFF: The Year in Digital Civil Liberties Cont.	DEF CON Comedy Inception: How many levels deep can we go? Cont.	I'm A Newbie Yet I Can Hack ZigBee - Take Unauthorized Control Over ZigBee Devices LI Jun & YANG Qing	Linux Containers: Future or Fantasy? Aaron Grattafiori

表 4：DEF CON 23 會議第 4 日議程(8 月 9 日)

Time	TRACK ONE	TRACK TWO	TRACK THREE	DEF CON 101
10:00	Abusing Adobe Reader's JavaScript APIs Brian Gorenc, Abdul-Aziz Hariri, Jasiel Spelman	Docker, Docker, Give Me The News, I Got A Bad Case Of Securing You David Mortman	How to Hack Government: Technologists as Policy Makers Terrell McSweeny & Ashkan Soltani	Abusing native Shims for Post Exploitation Sean Pierce
11:00	Who Will Rule the Sky? The Coming Drone Policy Wars Matt Cagle & Eric Cheng	Canary: Keeping Your Dick Pics Safe(r) Rob Bathurst (evilrob) & Jeff Thomas (xaphan)	REpsych: Psychological Warfare in Reverse Engineering Chris Domas	Ubiquity Forensics - Your iCloud and You Sarah Edwards
12:00	Knocking my neighbor's kid's cruddy drone offline Michael Robinson	Pivoting Without Rights - Introducing Pivoter Geoff Walton & Dave Kennedy	Stick That In Your (root)Pipe & Smoke It Patrick Wardle	Hijacking Arbitrary .NET Application Control Flow Topher Timzen
13:00	Attacking Hypervisors Using Firmware and Hardware Yuriy Bulygin	Why nation-state malwares target Telco Networks: Dissecting technical capabilities of Regin and its counterparts Omer Coskun	"Quantum" Classification of Malware John Seymour	RFIDiggity: Pentester Guide to Hacking HF/NFC and UHF RFID Francis Brown & Shubham Shah
14:00	Inter-VM data exfiltration: The art of cache timing covert channel on x86 multi-core Etienne Martineau	Let's Talk About SOAP, Baby. Let's Talk About UPNP Ricky "HeadlessZeke" Lawshae	Advances in Linux Process Forensics Using ECFS Ryan O'Neill	Contest Closing Ceremonies

15:00	Closed for Setup	Closed for Setup	Closed for Setup	Contest Closing Ceremonies Cont.
16:30	Closing Ceremonies	Closing Ceremonies	Closing Ceremonies	

二、重點議題

(一)Red vs. Blue: Modern Active Directory Attacks & Defense

主講者 Sean Metcalf 說明了如何在目錄服務(Active Directory)中取得維護管理存取權限的最新攻擊技術，以及描述如何偵測 Golden Ticket 的使用，以下為此次議程的演講重點：

1. MS14-068 漏洞的研究、利用以及危險性。
2. SPN 掃描：使用 PowerShell 工具來找出潛在的攻擊目標，而不是只使用於網路掃描(如：SQL、Exchange、FIM 以及 webservers 等)。
3. 利用服務帳戶的弱密碼，成為一個 AD 用戶。
4. Mimikatz(攻擊者的多功能工具) 。
5. 採用 Silver Tickets 的 Stealthy Persistence 的特性，將不會被偵測到。
6. 識別偽造的 Kerberos Ticket(Golden & Silver Tickets)。
7. 檢測像調用-Mimikatz 進攻的 PowerShell 工具。
8. 偵測 PowerShell 的攻擊。
9. 減緩 Active Directory 的攻擊。

從無到有的獲取 Domain Admin，必須利用以下幾點之特性：

1. 服務帳號的弱密碼 (Poor Service Account Passwords)
2. 密碼儲存於 Sysvol (Passwords in SYSVOL)
3. Credential 偷竊 (Credential Theft)
4. 錯誤設定(Misconfiguration / Incorrect Perms)
5. 利用已知漏洞(Exploit Vulnerability)

首先透過 PowerShell 所提供的 Find-PSServiceAccounts 功能，搜尋已經的服務帳號，詳見圖 1：

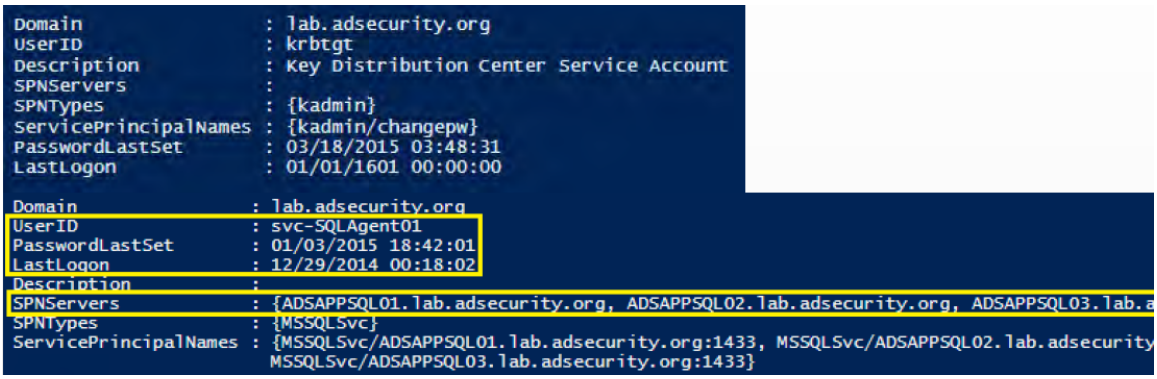


圖 1：SPN Scanning for Service Accounts with Find-PSServiceAccounts

再透過 tgsrepcrack.py 工具破解 TGS 服務的 Ticket(詳見圖 2)

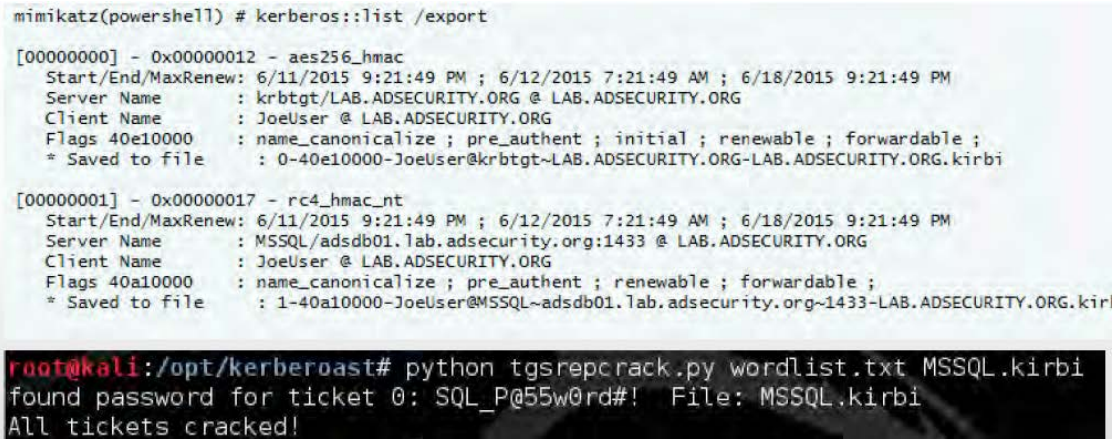


圖 2：Kerberoast: Save & Crack TGS Service Ticket

為了要達到 Credentials 偷竊的目的，可以利用 Mimikatz 工具進行 Dump Credentials，詳見圖 3。Mimikatz 除了可以 Dump Credentials，也能 Dump Kerberos Tickets、Credential 注入攻擊(Credential Injection)、產生 Silver/Golden Tickets 等。Dump AD 網域下的 Credentials 的特性如下：

- 於網域主控站(Domain Controller 簡稱 DC)上獲取 Credentials 資料 (local or remote).
  - 執行 Mimikatz (如：WCE) 於網域主控站(Domain Controller 簡稱 DC)。
  - 透過 PowserShell 遠端執行 Invoke-Mimikatz 於網域主控站上。
- 存取 NTDS.dit 檔案並取出資料

- 透過遠端網域主控站，複製 AD 資料庫。
- 從備份檔案上複製 AD 資料庫。
- 獲得虛擬的網域主控站資料。

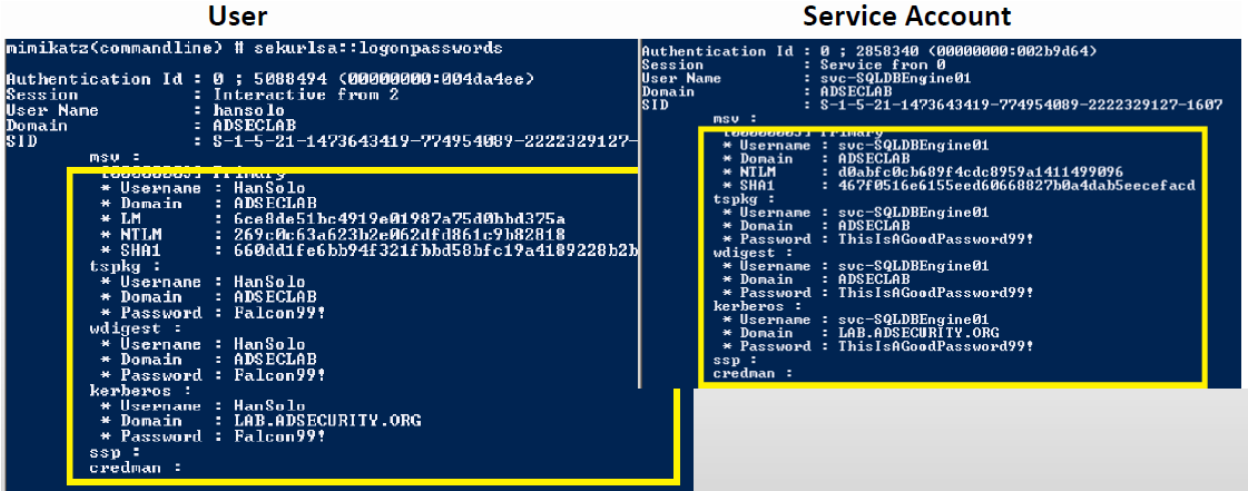


圖 3：Dump Credentials with Mimikatz User

若是網域主控站備份(DC backups)並沒有採用適當的保護措施，則攻擊者可能可以透過攻擊，從網路上獲取 NTDS.dit 檔案。

MS14-068 漏洞可允許攻擊者將未經授權的網域使用者帳戶權限，提高到網域管理員帳戶的權限。攻擊者可使用這些提高的權限入侵網域中的任何電腦，包括網域控制站。其造成的主因為網域主控站的 Kerberos 服務(Domain Controller Kerberos Service) (KDC) 無法正確的驗證其 PAC 的 Checksum。攻擊者必須擁有有效的網域認證，才能利用這項資訊安全風險。 擁有具備網域認證之標準使用者帳戶的使用者可從遠端使用受影響的元件。以下為建議措施：

1. 監控機敏系統的預定任務。
2. 阻擋網路存取網域主控站(DC)與伺服器。
3. 針對已知的假冒 Kerberos 與備份事件，監控所有伺服器的安全事件日誌。
4. 每年必須改變 KRBTGT 帳戶的密碼 2 次。或當一個 AD 管理者離開時改變其密碼。
5. 針對近期的資安事件，考量其威脅，並加入其威脅處理程序中與威脅模組中。

(二)QARK: Android App Exploit and SCA Tool

快速 Android 檢測套件(Quick Android Review Kit，簡稱 QARK)，QARK 是一個被設計為檢查 Android 行動軟體多項安全漏洞的工具，QARK 自動化的使用了多樣的反編譯工具，並整合其輸出結果。以下為 QARK 工具所能找出的問題：

1. 不經意對外的元件(Inadvertently Exported Components)
2. 不當保護的對外元件(Improperly Protected Exported Components)
3. 可能被攔截的 Intent(Intents which are Vulnerable to Interception or Eavesdropping)
4. 無效的 x.509 憑證(Improper x.509 Certificate Validation)
5. 全域可讀的檔案漏洞(Creation of World-readable or World-writeable files)
6. Activity 資料外洩(Activities which may Leak Data)
7. 使用 Sticky Intent(The Use of Sticky Intents)
8. 不安全的 Pending Intendts (\Insecurely Created Pending Intents)
9. 寄送不安全的廣播 Intents (Sending of Insecure Broadcast Intents)
10. 原碼洩漏金鑰(Private Keys Embedded in the Source)
11. 弱加密使用(Weak or improper Cryptography Use)
12. 潛在的 WebView 漏洞(Potentially Exploitable WebView Configurations)
13. 匯出偏好 Activities (Exported Preference Activities)
14. 觸屏挾持(Tapjacking)
15. 允許備份(Apps which Enable Backups)
16. 允許可調式(Apps which are Debuggable)
17. 支援過期的 API (Apps Supporting Outdated API Versions, with Known Vulnerabilities)

透過反編譯工具，從 APK 檔案萃取出 resources.arsc、/res、AndroidManifest.xml、classes.dex、/META-INF、/lib 以及/assets 等目錄與檔案，詳見圖 4：

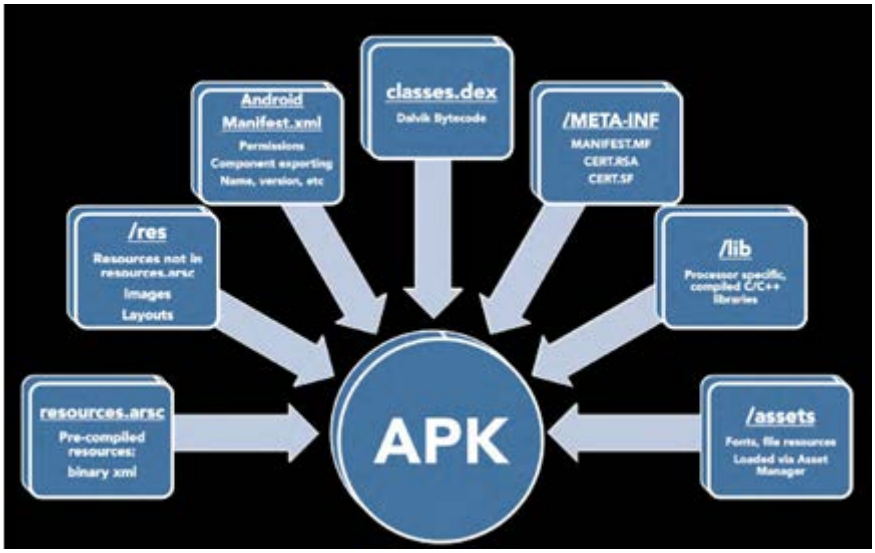


圖 4：APK Structure

針對 APK 檔案進行逆向工程之步驟為透過「apktool」工具將 APK 檔案進行反編譯並取得其 Manifest.xml 檔案，同時也針對 APK 進行解壓縮，取得 Dalvik Bycode 的檔案 classes.dex，透過「dex2jar」工具將 classes.dex 轉換成 jar 格式的檔案，最後透過 JD-GUI 工具針對 jar 檔案進行查看，即可檢視其 JAVA 語言的原始碼，其流程詳見圖 5：

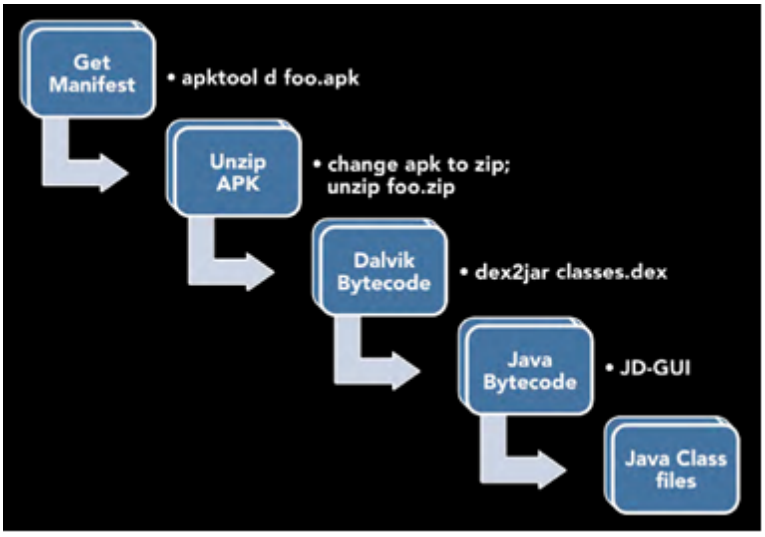


圖 5：Reversing APKs

利用反編譯後的資訊進行整理，檢視其 WebView 的設定、廣播 Intents、Sticky Intents、Pending Intents、全域可讀檔案、觸屏挾持漏洞以及 X.509 憑證有效性等。

最後將產生 HTML 格式的報告，供相關人員進行閱讀。

- Future Plans
  - 動態分析
  - 處理混淆原始碼(Obfuscated Code)
  - Smali 碼分析
  - 原生碼支援(Native Code Support)

(三) How To Shot Web

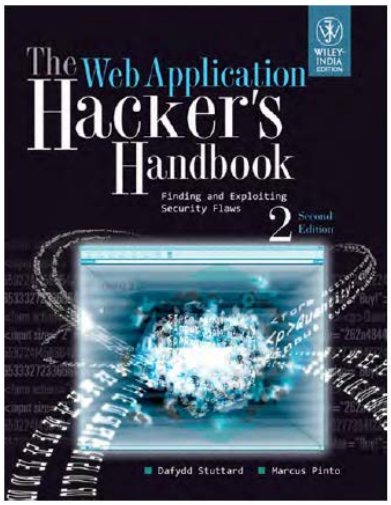
此議程描述了各式各樣的 WEB 攻擊手段，透過特別得滲透測試技巧，有助於在近年來得資安漏洞獎金計畫中(詳見圖 6)，獲得資安獎金。在演講過程中，介紹了攻擊理念、資料收集技巧、mapping 技術、Fuzzing、XSS、SQL 注入攻擊、CSRF 攻擊、網站服務以及行動安全漏洞等相關知識或技巧。在此議程中，透過吸收不同的滲透測試技術與技巧，有助於增加自己的滲透測試能力。

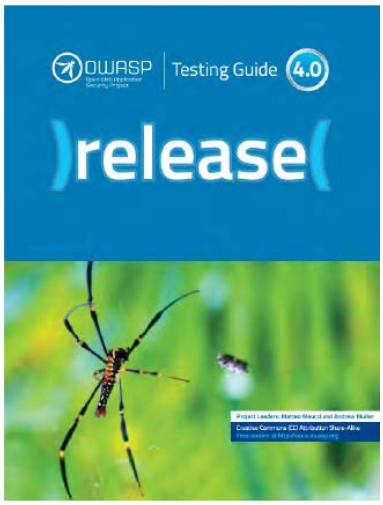
#	Acquisition date	Company	Business	Location	Value (USD)
1	August 23, 2005	facebook.com domain name	AboutFace	USA, Boston	$200,000
2	July 19, 2007	Parakey	Offline applications/Web OS	USA, Mountain View, CA	
3	June 23, 2008	ConnectU	Social networking	USA, Cambridge, MA	$31,000,000
4	August 10, 2009	FriendFeed	Social networking aggregator	USA, Mountain View, CA	$47,500,000
5	February 19, 2010	Octazen	Contact importer	Malaysia, Taman Melawati, Kuala Lumpur	

圖 6：Facebook 資安漏洞賞金計畫紀錄(資料來源：Wiki)

成為一名滲透測試人員之前，必須了解執行滲透測試相關的檢測流程、方法與漏洞評估方法，因此可以透過參考「The Web Application Hacker's Handbook」與「OWASP Testing Guide 4.0」(詳見圖 7)，了解執行滲透測試時得相關項目。不僅滲透測試人員可以透過此相關書籍，了解滲透測試之指引，開發人員也能透過其測試項目，在開發過

程中，就考量了相關的安全問題，降低維護成本。





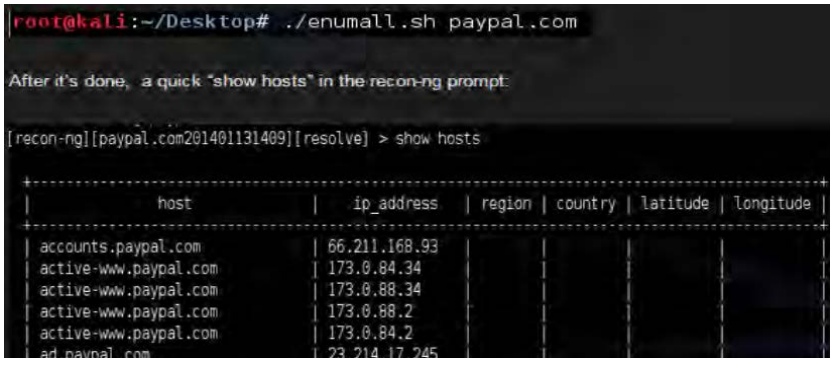
資料來源：OWASP / Dafydd Stuttard, Marcus Pinto

圖 7：Testing Guide & Hacker Handbook

在開始執行滲透測試前，須先收集受測目標相關資料，常見的資料蒐集方法如下：

1. Google 搜尋。
2. Port 掃描。
3. 確認受測目標是否有提供漏洞獎金。
4. 行動版的網站也可納入目標。
5. 受測目標是否有提供行動軟體。
6. 觀察 DNS。

透過 enumall.sh 工具，能夠列舉出網站的相關資料(詳見圖 8)：



資料來源：OWASP / Dafydd Stuttard, Marcus Pinto

圖 8：Enumall.sh 指令列舉網站資訊

在通訊埠(Port)掃描的部分，其技巧如下：

- 針對個別的網站進行掃描
- 可觀察對於網站本身外來的服務
- Syn scan
- OS + service fingerprint
- 不使用 ping
- 全部的 Port
- http titles

在針對網站進行掃描時，可以透過字典暴力破解的方式，嘗試挖掘網站結構。針對 401 有反應的 URL，應該要持續得進行挖掘，詳見圖 9：

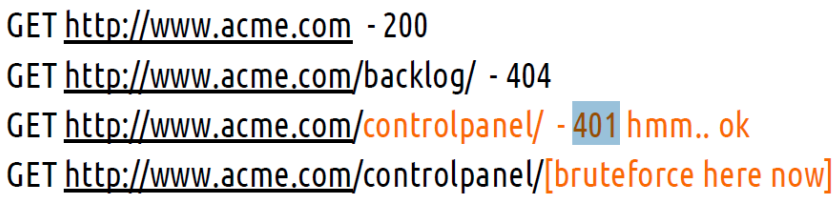


圖 9：字典暴力破解流程

即使某類型的漏洞已經被揭露，但可能在不同功能下發現同類型或是些許變化的漏洞，因此透過參考過去的漏洞，仍然有很大的機會能夠持續發現相似的漏洞，詳見圖 10：

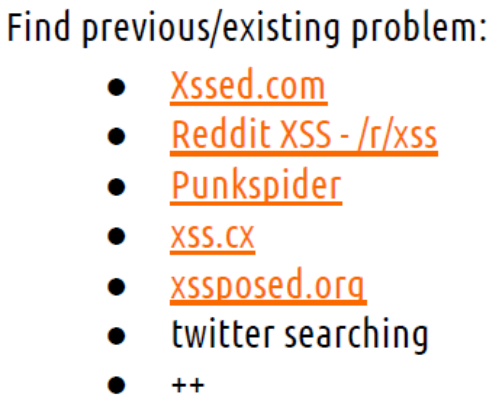


圖 10：查詢並整理網站過去漏洞的紀錄

在認證機制方面，註冊頁面往往是攻擊的入口點，因此首先針對帳戶登入時的錯誤

訊息進行觀察，是否在執行特定的輸入，能夠挖掘資訊，或是針對登入成功後的頁面進行觀察，在 Session 管理方面是否完善，其他觀察重點如：密碼重設頁面、是否有無帳號鎖定機制、弱密碼政策、定期更新密碼政策等。在 Session 管理重點如下：

1. 可注意是否針對過期 Cookie 進行驗證。
2. Cookie 的 Timeout 策略。
3. Cookie 長度限制。
4. 多重 Cookie 的管理。
5. Cookie 的複雜度是否穩固。

XSS 是一種常見的攻擊，針對常見的攻擊向量如下：

1. URL Based
2. JSON POST 的值
3. 上傳檔案(SWF 與 HTML 等)
4. 特製的錯誤頁面
5. 假參數
6. 登入或忘記密碼頁面

在 SQL 注入攻擊方面，可透過 Burp Suite 使用 SQLmap SQLiPy 功能，針對網站進行 SQL 注入攻擊，大大的提升漏洞挖掘的效率，詳見圖 11：

圖 11：Burp Suite - SQLmap SQLiPy

在惡意檔案上傳方面，惡意檔案上傳是一種容易讓開發人員疏忽的攻擊手段，因此

攻擊者可以透過以下技巧，利用惡意檔案上傳進行攻擊：

1. 上傳檔案的格式限制(ShellCode)
2. 檔案內容為 XSS 語法攻擊
3. DOS 攻擊
4. 上傳 malware，等待被執行

綜合以上相關內容，可以得到的初步結論如下：

1. Crowdsourced 測試注重在快速
2. 資料分析往往是成功達成攻擊的關鍵
3. 在 15 分鐘的網站測試中，必須大量的檢視關鍵的漏洞
4. 須使用強大與整合式的掃描套件
5. 需要週期性的更新攻擊手法

(四) Remote exploitation of an unaltered passenger vehicle

Wired 網站編輯 Andy Greenberg 與兩名資安研究人員 Charlie Miller 與 Chris Valasek，於 7 月 21 日在網站發布一項 Fiat Chrysler 車載系統遠端入侵實驗結果。兩名研究人員從遠端操控了 Greenberg 所駕駛的飛雅特克萊斯勒 (Fiat Chrysler) 吉普車，從空調、音響、雨刷、油門到剎車，甚至還造成吉普車剎車失靈滑向停車場邊的草地。飛雅特克萊斯勒開發一款名為 Uconnect 的車載資訊娛樂系統 (In-Vehicle Infotainment, IVI)，提供娛樂、手機連結、導航、語音命令與控制功能，還有一項 Uconnect Access Via Mobile 服務，允許駕駛利用手機的數據服務存取支援 Uconnect 的行動程式。Uconnect 可安裝在該品牌旗下的汽車、吉普車，或卡車上。而 Miller 與 Valasek 則找到 Uconnect 的安全漏洞進行攻擊。

當 Greenberg 的吉普車行駛在道路上時，冷氣忽然自動開到最大，音響自動轉到當地的嘻哈電台且切換至最大音量，然後雨刷也自動啟用，還看到 Miller 與 Valasek 的照片出現在汽車的顯示器上，甚至關閉引擎。接著當車到停車場時，研究人員還切斷了吉普車的油門，造成吉普車突然失速，最後還讓車子剎車失靈，使得吉普車失控滑向一旁的草地。這兩名研究人員先改寫了 Uconnect 上的晶片韌體，以讓韌體得以接收並傳送命

令至不同的汽車零件。Uconnect 在美國是經由 Sprint 電信網路傳輸，在研究人員掃描 Sprint 網路之後，估計路上約有 47.1 萬台汽車採用不安全的 Uconnect 系統。

他們在 2014 年 10 月便把相關漏洞提報給業者，飛雅特克萊斯勒也已經於 2015 年 7 月釋出修補程式。研究人員則在會議上揭露更詳細的漏洞細節。車載資訊娛樂系統的安全性最近愈來愈受到重視，研究人員也陸續展示攻陷 IVI 的技術與手法，多半都是可以自遠端操控汽車內部的各種元件，也能追蹤汽車的動向。對此美國參議員 Edward Markey 與 Richard Blumenthal 在 2015 年 7 月共同提出一項車載系統安全暨隱私法案 (Security and Privacy in Your Car, SPY Car)(完整 SPY Car 提案內容請參閱：http://www.markey.senate.gov/imo/media/doc/SPY%20Car%20legislation.pdf)，希望能建立保障汽車安全及保護駕駛隱私的聯邦標準，並透過分級系統來讓消費者了解汽車的安全保障能力。Markey 說，人們需要清楚的道路規定來保護汽車不受駭客的攻擊，同時保障美國家庭的隱私，此一法案將建立最低的標準與清楚的規範以在連網汽車漸增的時代保護駕駛的資料、安全及隱私。

(五) Stagefright: Scary Code in the Heart of Android

資安公司 Zimperium 前於 7 月 27 日在官方部落格發布消息，其研究團隊發現有一個重大的安全漏洞，存在於幾乎所有版本的 Android 作業系統，只要傳一封惡意簡訊就能造成用戶被駭，讓 95%的 Android 智慧型手機皆曝露在風險中，因而被認為這是迄今被發現最危險的 Android 漏洞。Zimperium 的安全研究人員 Joshua J. Drake，在 Android 處理多種常見媒體格式的媒體函式庫 Stagefright 內，發現一個遠端程式碼執行漏洞。該公司於美國的駭客大會 Black Hat 及 DEF CON 23 公佈這項漏洞的細節，主要是這個以 C++ 程式語言實作的函式庫比其他以 Java 程式語言寫成的函式庫更容易出現記憶體毀損。

Stagefright 中的漏洞可讓駭客經由多種不同方法入侵 Android 裝置，跟以往 Android 漏洞最大的不同點在於，過去的 Android 攻擊均需要用戶自行安裝 APP 才能成功入侵，但利用這個 Android 漏洞，駭客不用和用戶有任何互動就可發動攻擊，而且攻擊者還能消除所有攻擊痕跡，讓用戶難以查覺遭木馬程式感染而持續使用手機。在最嚴重的攻擊途徑中，攻擊者只需要知道用戶手機號碼，經由多媒體簡訊 (Multimedia

Messaging Service, MMS) 傳送變造過的惡意檔案，即可入侵用戶手機，並遠端執行程式碼。精心設計的攻擊甚至能在使用者看到訊息前將之刪除，用戶只會看到訊息通知。

Google 在接獲 Zimperium 通報後，已於 48 小時內製作並發布 Nexus 手機版本之修補程式。然而由於 Android 版本相當分散，要將所有版本及不同手機廠商的作業系統修補完成將相當困難。Zimperium 指出，修補漏洞需要升級韌體，但一般 18 個月以上的行動裝置幾乎完全無法得到廠商的更新支援。Zimperium 呼籲用戶或企業應儘速聯絡手機廠商或電信業者，以了解自身的手機是否已有更新。

肆、心得建議

資通訊科技與網際網路蓬勃發展，已改變人類之生活模式，也帶來日益嚴重與多樣化之資安威脅。未來，隨大數據、智慧聯網、移動裝置及雲端服務等新興資通訊科技應用普及，網路與實體世界逐漸融合，資安對於民眾生活、經濟活動、國家安全影響加鉅，近年先進國家除在資安防護上投入大量資源，也透過立法手段，加強資安作為並宣示資安為國家在數位時代發展之重要基石。行政院資通安全辦公室已參酌國際先進國家立法原則，考量我國社經環境與法規制度等，完成「資通安全管理法(草案)」之研議，擬透過國家資安政策之落實及資安環境之加速建構，同步提升公務機關、非公務機關及資安產業整體能量，以確保民眾數位生活福祉、新興資安產業發展及數位國土國家安全。

因應資安威脅情勢日趨嚴峻，及政府、產業對資安人才需求日殷，行政院已規劃在「國家資通訊安全發展方案(102 年至 105 年)」推動基礎上，由行政院資通安全會報「認知教育及人才培育組」之主辦機關教育部會同科技部、經濟部等共同強化我國資安人才培育事宜。依行政院本年 5 月 13 日核定之「我國資安人才培育規劃」，我國資安人才培育目標為「向上厚植求質精、向下普植求量足」，並依人才培育之深度及廣度，分「資安菁英的培訓」、「目標導向的菁英教育」、「資安融入資通訊學門教育」及「向下扎根的資安認知教育」等層次推動。相關機關刻正透過「課程」、「平臺」、「競賽」、「實習」及「產學合作」等五大主軸，協力擴大資安人才培育，落實訓用合一；所需經費本年、105 年由相關機關勻支，106 年度起擬爭取政策額度科技預算，以擴大推動辦理各主軸重點工作。

本次 DEF CON 的 CTF 競賽最終由韓國代表隊 DEFKOR 以極大的差距拿下冠軍，該隊主要係韓國近年來積極推動資安菁英人才培育計畫(Best of Best, BoB)，所培訓出來的菁英隊伍；至於代表我國的 HITCON 實力雖成長不少，但其他國家的代表隊實力亦不容小覷，最終 HITCON 獲得第 4 名的佳績。此外，值得一提的是美國國防部(DARPA)於 DEF CON 舉辦的 Cyber Grand Challenge 比賽，參賽隊伍必須設計出一台能自動尋找及修補漏洞，甚至可以自動撰寫攻擊程式的機器，入圍的團隊除了由 DARPA 提供資金贊助外，獲得冠

軍隊伍將可獲得 200 萬美金的獎金，並於明(2016)年的 DEF CON 中，與世界各國代表隊共同參加 CTF 競賽，屆時，駭客與機器之間的攻防戰將是比賽注目的焦點，同時也將網路攻防領域提升至另一個層次。

伍、會議照片

圖 15：會議地點

圖 16：排隊購買門票現況

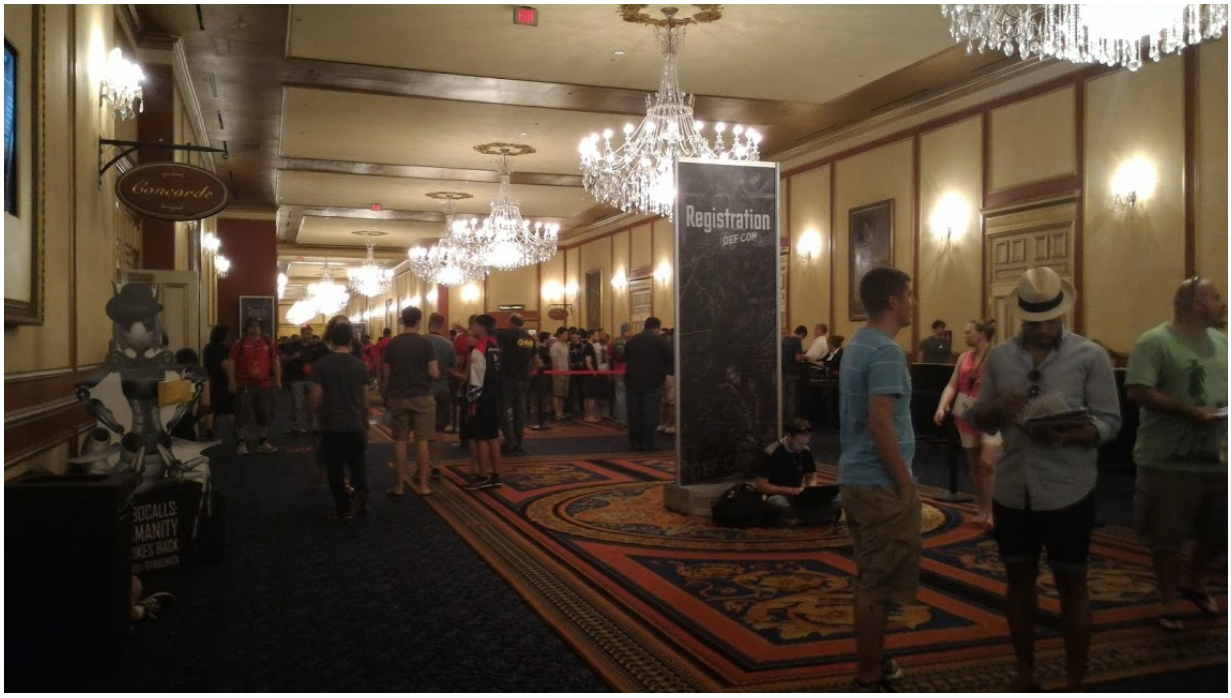


圖 16：會議報到處

圖 17：會議識別證及手冊

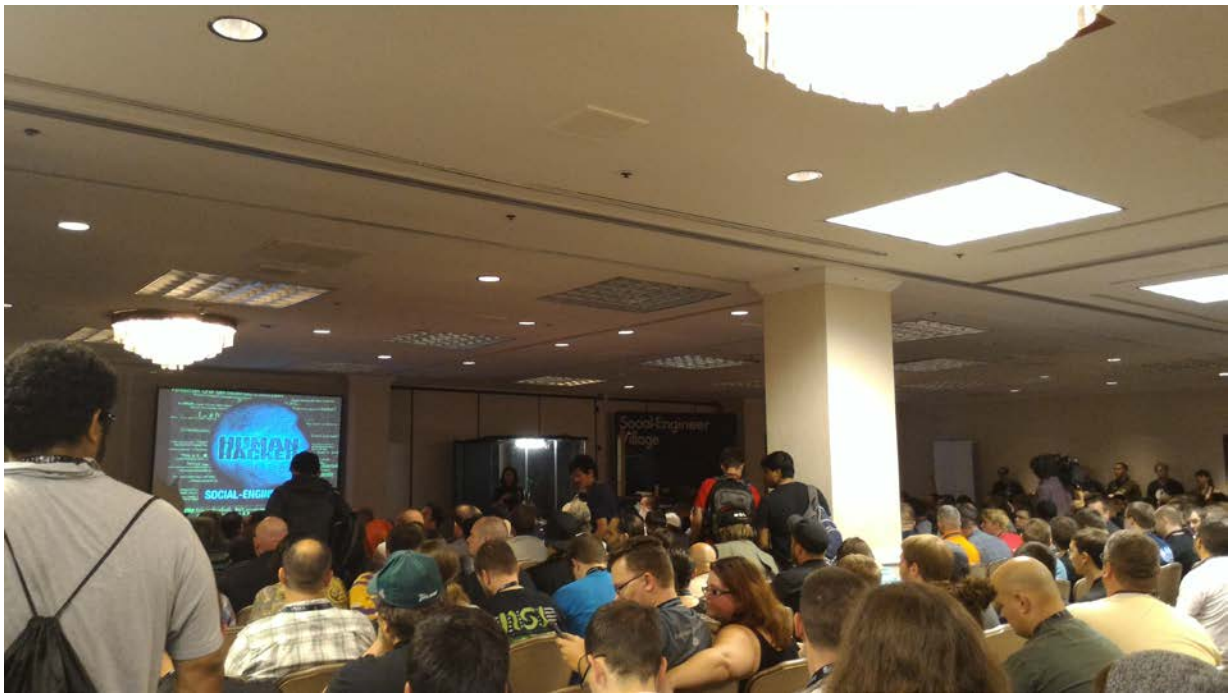


圖 18：Social Engineering Village 現場

圖 19：會議休息區

圖 20：廠商展示區

圖 21：ICS Village 現場

圖 22：Car Hacking Village(現場展示 Tesla 車款供駭客入侵測試)

圖 23：網路攻防競賽(Capture the Flag, CTF)現場

圖 24：CTF 我國參賽代表隊(HITCON)

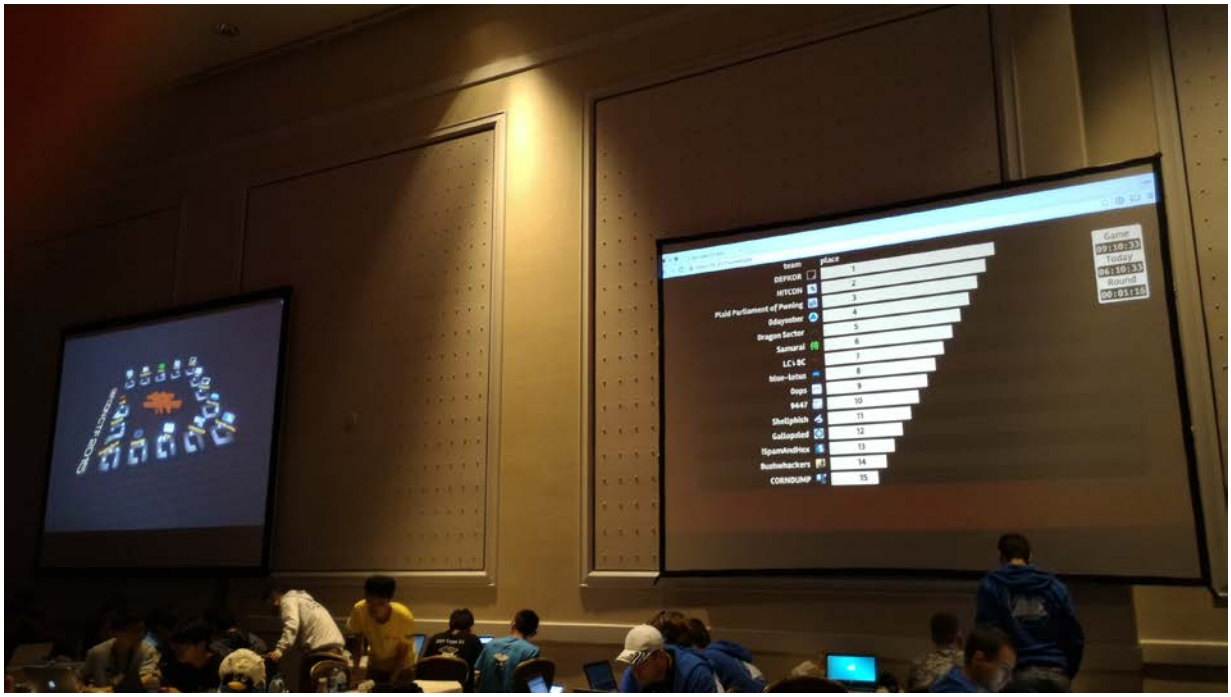


圖 25：CTF 比賽現況(左邊為攻擊現況圖，右圖為排行榜)

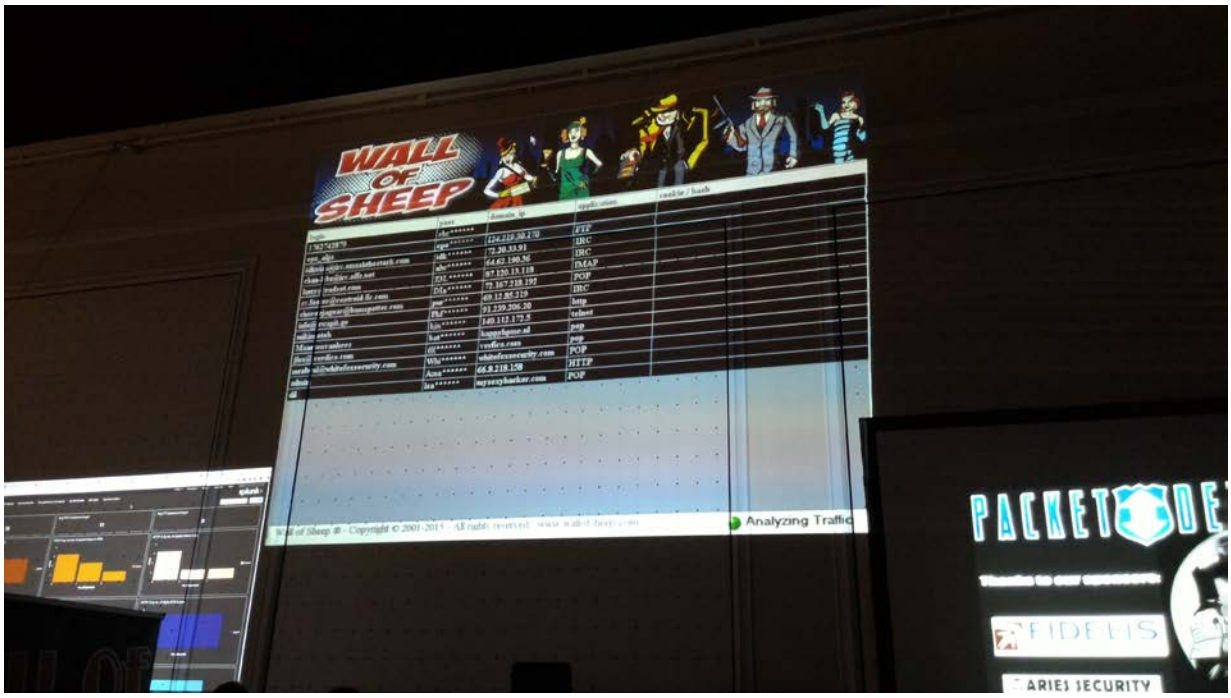


圖 26：綿羊牆(Wall of Sheep)

圖 27：閉幕會議