



2007 年駭客年會徵求論文

HIT 2007 Call For Paper

- ◆ 時間: 2007 年 7 月 21 日~22 日 (星期六~星期日)
- ◆ 主辦單位: CHROOT — Security Research Group (<http://www.chroot.org>)
- ◆ 活動網址: <http://hitcon.org>

台灣第三屆駭客年會將於 2007 年 7 月 21~22 日 (週六、日) 舉行, 歡迎各界人士踴躍投稿。論文內容以探討實作技術並能演講 50 分鐘為佳。

為了讓會議主題能夠明確, 我們擬定了以下議題, 有興趣的朋友可以從下列議題中選擇自己擅長的方面進行準備(包括論文、程式碼和投影片), 但不以下列的議題為限。今年特別歡迎各項有關 Windows Vista 作業系統的安全技術探討。

1. Exploit technique
對於網路、作業系統和應用程式等各方面攻擊程式或手法的技術研究。
2. Honeypot
構建安全的 Honeynet 系統, 對各種入侵進行詳細的技術分析, 瞭解攻擊者行為和攻擊手法等。或者, 對於 Honeypot 進行反追蹤技術的探討。
3. Virus and anti-virus
電腦病毒和防毒軟體新趨勢或研究。
4. Reverse engineering
對二進位檔或者不明資料進行詳細解析, 構建反向工程的具體過程和方法。
5. Audit software vulnerability
對開放原始碼的軟體進行安全性檢測與分析的具體過程和方法, 或是對商業軟體所進行的安全性分析。
6. Backdoor and rootkit
各種新型態的後門或木馬的設計研究或是檢查方式。
7. Web and database security
各種網頁、網站軟體和資料庫的安全性探討。
8. Firewall, WAF, IDS and IDP
防火牆(Firewall)、入侵偵測(防禦)系統(IDS、IDP)等的技術現狀和發展前景, 入侵檢測系統在現階段的實際應用情況等。此外, 歡迎近年來對於加強 Web 應用程式安全的 WAF (Web Application Firewall)的各項技術研究。
9. Hardened system
對各種當前各種作業系統進行安全加強, 提升不同安全級別方法、技術、發展方向等。
10. Covert Channel
隱藏傳輸通道。將某特定的資料隱藏包裝於其它正常的資料串流或協定中, 進行傳送。

論文可選中文或英文撰寫。每文第一頁必須包含題目、作者、聯絡人、演講者及聯絡資料(電話、電子郵件)等, 並以 PDF 檔格式, 於 2007 年 6 月 15 日前, 利用電子郵件附帶傳送檔案至 hit2007@hitcon.org。

為鼓勵投稿, 本次會議將致贈每篇被接受之論文 NT \$3,000 元整。此外, 大會將依作者意願, 將論文或演講內容以電子或書面媒體方式散佈。

除了上述的論文徵求外, 本次駭客年會計畫了一場 0-day exploit 展示, 只要在 2006 年 7 月 15 日前, 將您個人所發現的漏洞(未公開且尚未被修正), 以電子郵件方式傳送至 hit2007@hitcon.org, 經過確認, 就有機會免費取得本屆駭客年會的入場券, 並且上台展示漏洞。