

NAR Labs 國家實驗研究院

國家高速網路與計算中心

Kali Linux 滲透測試實務

講師：蔡一郎

助教：許清雄

Google Me.

- 蔡一郎 Steven
- 學歷：國立成功大學電腦與通訊工程研究所
- 現任：財團法人國家實驗研究院 國家高速網路與計算中心 副研究員
- 重要經歷：
 - 國立成功大學研究發展基金會 助理研究員
 - 中華民國資料保護協會 1st 監事
 - 中華民國南部科學園區產學協會 5th 理事、6th 監事
 - 台灣科技化服務協會 3rd 理事
 - 台灣雲端安全聯盟 1st 理事長
 - 台灣資訊安全聯合發展協會 1st 常務監事
 - The Honeynet Project Taiwan Chapter Leader
 - Cloud Security Alliance Taiwan Chapter Founder and Director of Research
 - 部落客：<http://blog.yilang.org>
 - Facebook: Yi-Lang Tsai
 - 自由作家
 - 電腦圖書著作34本
 - Information Security(資安人)、Linux Guide、NetAdmin、網路資訊等文章，計80餘篇
- 專業證照：
 - RHCE、CCNA、CCAI、CEH、CHFI、ACIA、ITIL Foundation、ISO 27001 LAC、ISO 20000 LAC、BS10012 LAC、CSA STAR



AboutMe

- 許清雄 Stan < chingshiung@narlabs.org.tw >
- 學歷：大葉大學資訊工程學系
- 現任：
 - 國家高速網路與計算中心 專案佐理工程師
 - The Honeynet Project Taiwan Chapter Contributor
 - RAT Core Members
- 經歷：
 - Honeycon2013 講師
 - 台中二十號倉庫 網管工程師
- 興趣：
 - 專研駭客攻擊手法



Agenda

- 滲透測試介紹
- Kali Linux 介紹
- 建立滲透測試環境
- 偵查
- 掃描
- 密碼破解

課程目標

- 本課程的目標在於透過實際應用，讓學員可以瞭解滲透測試之目的以及流程，並掌握其所需之相關技巧。



注意事項

- 課程期間，請對指定範圍內的資訊設備進行測試。
- 課程結束後，使用任何網路攻擊技巧對任何資訊設備進行攻擊皆屬個人行為。
- 請勿違反本國電腦犯罪相關法令！

國內電腦犯罪相關法令

- 刑法第36章妨礙電腦使用罪
 - 第358條
 - 無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而侵入他人之電腦或其相關設備者，處3年以下有期徒刑、拘役或科或併科10萬元以下罰金。
 - 第359條
 - 無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。

國內電腦犯罪相關法令

- 刑法第36章妨礙電腦使用罪
 - 第360條
 - 無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
 - 第361條
 - 對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。
 - 第362條
 - 第358條至第360條之罪，須告訴乃論。

滲透測試

- 滲透測試(Penetration Test，簡稱PT)是委託專業的資安人員，以模擬外部攻擊者的方式，進行特定系統的攻擊以及入侵，藉此進行單位內的系統安全評估。
- 滲透測試可以使用網路探測、弱點掃描、社交工程…等手法。

滲透測試的目的

- 實現系統漏洞所帶來的實際威脅以及風險。
- 提供系統漏洞資訊與攻擊難度給受測單位進行完整的風險評估
- 掌握最新的攻擊手法
- 除了系統安全，組織內成員的資安意識，與實體安全一樣都很重要

滲透測試的類型

- White-box testing
 - 與受測單位的代表一同進行測試。測試前充分掌握內部情報，針對單位內系統進行廣泛的弱點探測與評估。缺點為由於是在受控制的環境中進行，所以無法確認緊急應變系統是否有效運作。
- Black-box testing
 - 完全模擬由外部攻擊者進行入侵，可以同時測試系統安全以及緊急應變程序，但是測試難度較高。
- Grey-box testing
 - White-box+Grey-box

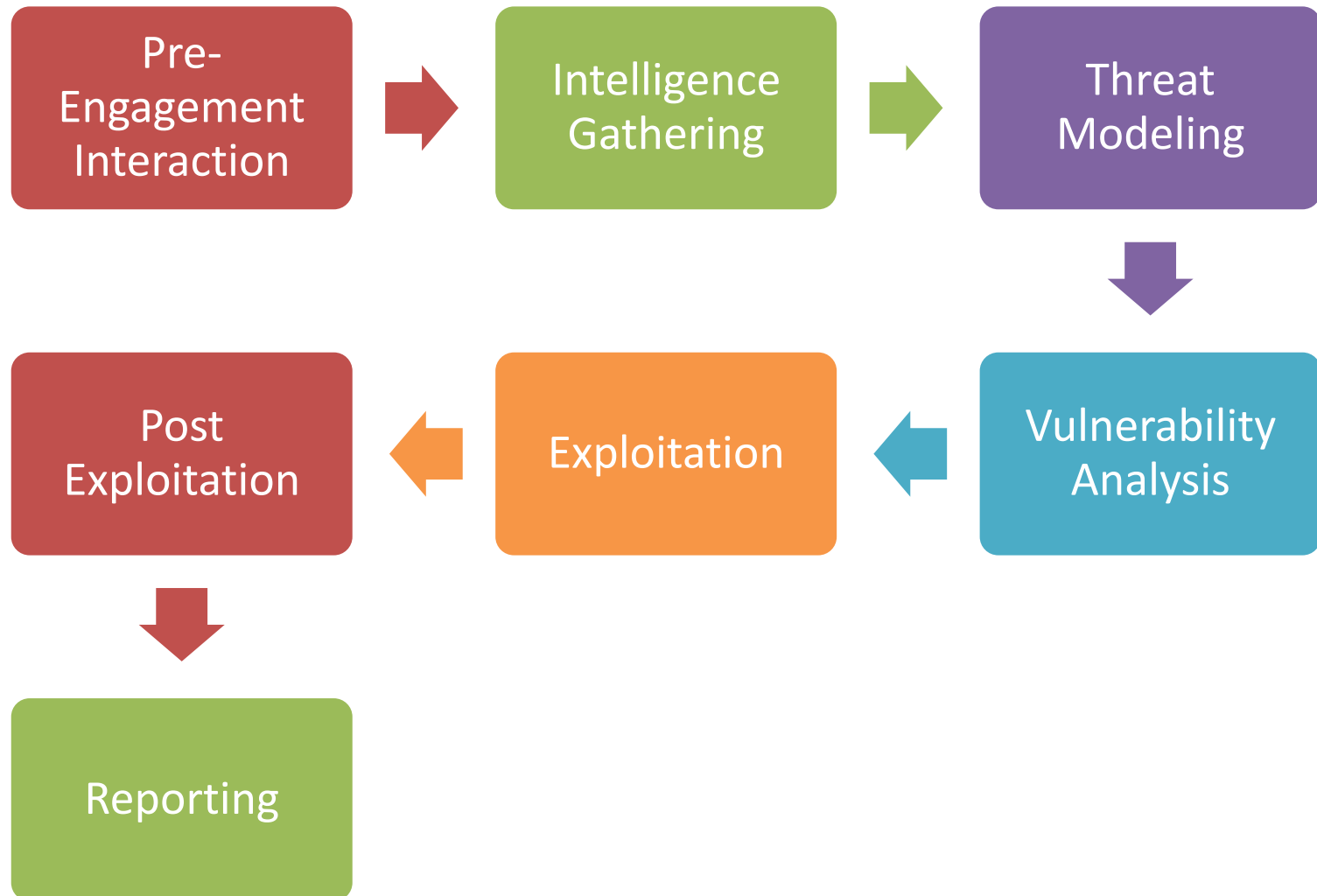
滲透測試的方法



滲透測試參考的標準與準則

- The Penetration Testing Execution Standard (簡稱PTES)
 - http://www.pentest-standard.org/index.php/Main_Page
- Open Source Security Testing Methodology Manual(簡稱OSSTMM)
 - <http://www.isecom.org/research/osstmm.html>
- Open Web Application Security Project(簡稱OWASP)
 - https://www.owasp.org/index.php/Main_Page

滲透測試的流程



Crack With Hacker



駭客入侵五大步驟

- 偵查
- 掃描
- 獲得存取
- 維持存取
- 湮滅蹤跡

情報收集

- Intelligence Gathering
 - Target selection
 - 目標選擇
 - Open Source Intelligence(OSINT)
 - 蒐集公開情報
 - Covert gathering
 - 秘密地進行主動測試並蒐集情資
 - Human Intelligence(HUMINT)
 - 透過人員訪談，找出可能的情資
 - Identify Protection Mechanisms
 - 辨識防護機制

威脅定義

- Threat Modeling
 - Business asset analysis
 - 企業資產分析
 - Business process analysis
 - 企業流程分析
 - Threat analysis
 - 威脅分析
 - Finding relevant news of comparable organizations being compromised
 - 他山之石可以攻錯

駭客入侵五大步驟 [✓]

- 偵查
- 掃描
- 獲得存取
- 維持存取
- 湮滅蹤跡

弱點分析

- Vulnerability Analysis
 - Active Testing
 - 主動測試
 - Passive Testing
 - 被動測試
 - Public research
 - 利用公開的系統漏洞資訊
 - Personal research
 - 模擬目標系統，嘗試找尋潛在漏洞
 - Validation
 - 關聯性分析與驗證

駭客入侵五大步驟 [✓]

- 偵查
- 掃描
- 獲得存取
- 維持存取
- 湮滅蹤跡

漏洞攻擊

- Exploitation
 - Ensure counter measurement bypass
 - 繞過現有資安機制
 - Customized exploitation avenue
 - 客製化的攻擊手法
 - Detection bypass
 - 必須要躲過偵測系統
 - Type of attacks
 - 選擇攻擊手法

系統滲透

- Post Exploitation
 - Infrastructure analysis
 - 完整的組織架構分析
 - High value targets
 - 確認高價值目標
 - Business impact attacks
 - 評估滲透後可以造成的企業衝擊規模
 - Cleanup
 - 清除足跡與相關事證
 - Persistence
 - 確保控制權

駭客入侵五大步驟 [✓]

- 偵查
- 掃描
- 獲得存取
- 維持存取
- 湮滅蹤跡

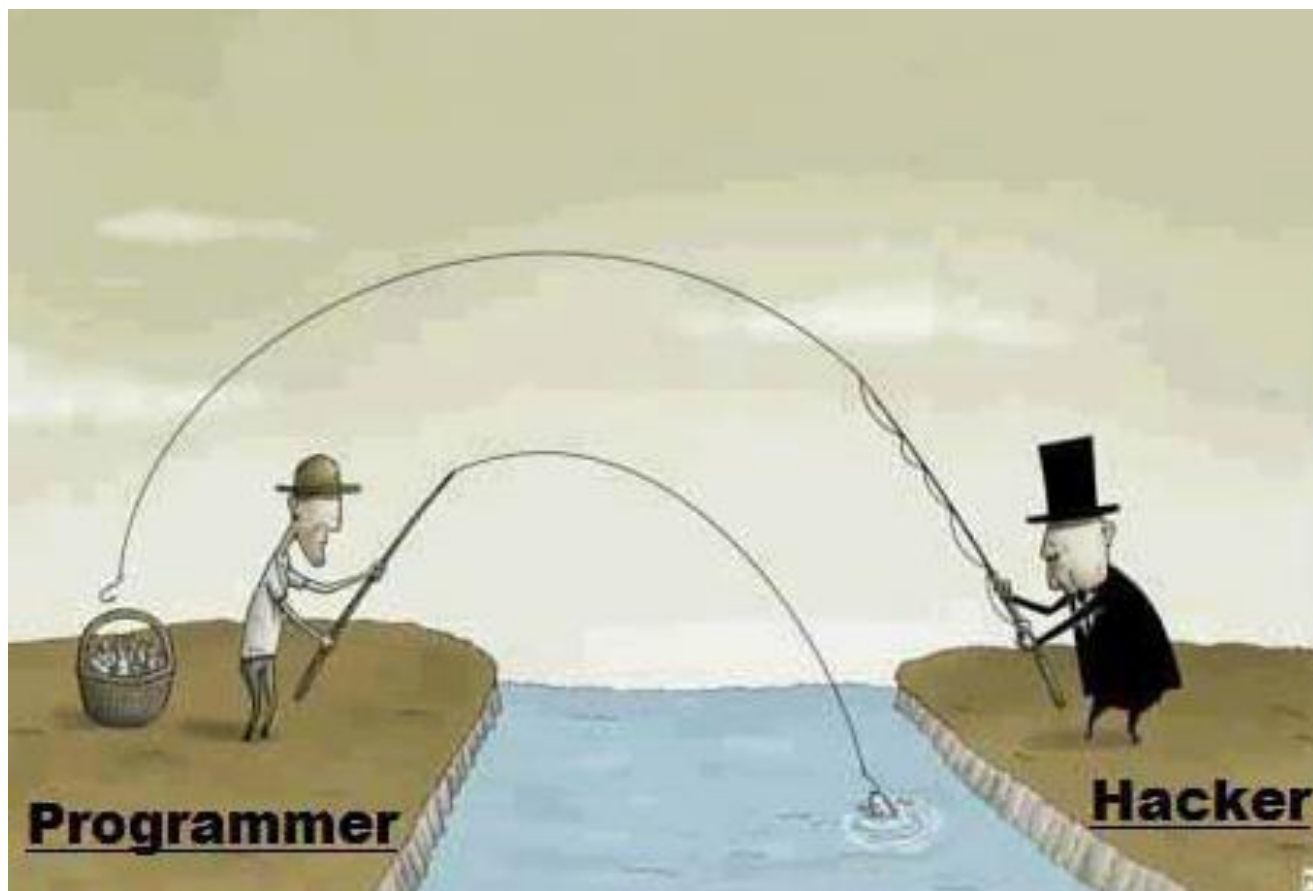
清除相關Log

```

2008-10-09 00:37:37.011 - 21384 12764 Sw_MessageHandler::Open - - - - 5 65535 "Initialization complete."
2008-10-09 00:37:39.152 CHSVSR07 21384 12764 Sw_SQLDataConnection::Open - - - - 2 41494 "Failed to establish a connection to the data source: (Server: CHSSQL01, Database:
2008-10-09 00:37:39.168 CHSVSR07 21384 12764 Sw_SQLOutputHandler::Open - - - - 1 44910 "Failed to connect to data source."
2008-10-09 00:37:39.558 - 18568 18792 Sw_MessageHandler::Open - - - - 5 65535 "Initialization complete."
2008-10-09 00:37:39.617 - 18900 20176 Sw_MessageHandler::Open - - - - 5 65535 "Initialization complete."
2008-10-09 00:37:39.668 - 21572 17944 Sw_MessageHandler::Open - - - - 5 65535 "Initialization complete."
2008-10-09 00:37:40.308 CHSVSR07 18900 20176 Sw_SQLDataConnection::Open - - - - 2 41494 "Failed to establish a connection to the data source: (Server: CHSSQL01, Database:
2008-10-09 00:37:40.308 CHSVSR07 18900 20176 Sw_SQLOutputHandler::Open - - - - 1 44910 "Failed to connect to data source."
2008-10-09 00:37:40.996 CHSVSR07 21572 17944 Sw_SQLDataConnection::Open - - - - 2 41494 "Failed to establish a connection to the data source: (Server: CHSSQL01, Database:
2008-10-09 00:37:41.012 CHSVSR07 21572 17944 Sw_SQLOutputHandler::Open - - - - 1 44910 "Failed to connect to data source."
2008-10-09 00:37:41.215 CHSVSR07 18568 18792 Sw_SQLDataConnection::Open - - - - 2 41494 "Failed to establish a connection to the data source: (Server: CHSSQL01, Database:
2008-10-09 00:37:41.215 CHSVSR07 18568 18792 Sw_SQLOutputHandler::Open - - - - 1 44910 "Failed to connect to data source."
2008-10-09 00:37:41.980 CHSVSR07 21384 12764 Sw_SystemDispatcher::Init - - - - 0 44951 "Successfully started Microsoft System Center Application Virtualization Management
2008-10-09 00:56:32.214 CHSVSR07 21384 12764 Sw_SystemDispatcher::Init - - - - 0 44952 "Successfully shut down Microsoft System Center Application Virtualization Manage
2008-10-09 00:56:32.292 CHSVSR07 21384 12764 Sw_MessageHandler::Close - - - - 5 65535 "Shutdown complete."
2008-10-09 00:56:32.573 CHSVSR07 18568 18792 Sw_MessageHandler::Close - - - - 5 65535 "Shutdown complete."
2008-10-09 00:56:32.573 CHSVSR07 18900 20176 Sw_MessageHandler::Close - - - - 5 65535 "Shutdown complete."
2008-10-09 00:56:32.573 CHSVSR07 21572 17944 Sw_MessageHandler::Close - - - - 5 65535 "Shutdown complete."
2008-10-09 00:58:37.375 - 1140 1164 Sw_MessageHandler::Open - - - - 5 65535 "Initialization complete."
2008-10-09 00:58:41.250 CHSVSR07 1140 1164 Sw_SQLDataConnection::Open - - - - 2 41494 "Failed to establish a connection to the data source: (Server: CHSSQL01, Database: S
2008-10-09 00:58:41.265 CHSVSR07 1140 1164 Sw_SQLOutputHandler::Open - - - - 1 44910 "Failed to connect to data source."
2008-10-09 00:58:41.765 - 1492 1496 Sw_MessageHandler::Open - - - - 5 65535 "Initialization complete."
2008-10-09 00:58:41.781 - 1512 1516 Sw_MessageHandler::Open - - - - 5 65535 "Initialization complete."
2008-10-09 00:58:41.781 - 1504 1508 Sw_MessageHandler::Open - - - - 5 65535 "Initialization complete."
2008-10-09 00:58:43.234 CHSVSR07 1512 1516 Sw_SQLDataConnection::Open - - - - 2 41494 "Failed to establish a connection to the data source: (Server: CHSSQL01, Database: S
2008-10-09 00:58:43.234 CHSVSR07 1504 1508 Sw_SQLDataConnection::Open - - - - 2 41494 "Failed to establish a connection to the data source: (Server: CHSSQL01, Database: S
2008-10-09 00:58:43.234 CHSVSR07 1512 1516 Sw_SQLOutputHandler::Open - - - - 1 44910 "Failed to connect to data source."
2008-10-09 00:58:43.234 CHSVSR07 1504 1508 Sw_SQLOutputHandler::Open - - - - 1 44910 "Failed to connect to data source."
2008-10-09 00:58:43.359 CHSVSR07 1492 1496 Sw_SQLDataConnection::Open - - - - 2 41494 "Failed to establish a connection to the data source: (Server: CHSSQL01, Database: S
2008-10-09 00:58:43.359 CHSVSR07 1492 1496 Sw_SQLOutputHandler::Open - - - - 1 44910 "Failed to connect to data source."
2008-10-09 00:58:46.328 CHSVSR07 1140 1164 Sw_SystemDispatcher::Init - - - - 0 44951 "Successfully started Microsoft System Center Application Virtualization Management S
2008-10-09 01:15:25.292 CHSVSR07 1140 1164 Sw_SystemDispatcher::Init - - - - 0 44952 "Successfully shut down Microsoft System Center Application Virtualization Management
2008-10-09 01:15:25.370 CHSVSR07 1140 1144 Sw_MessageHandler::Close - - - - 5 65535 "Shutdown complete."
2008-10-09 01:15:25.494 CHSVSR07 1492 1496 Sw_MessageHandler::Close - - - - 5 65535 "Shutdown complete."
2008-10-09 01:15:26.632 CHSVSR07 1512 1516 Sw_MessageHandler::Close - - - - 5 65535 "Shutdown complete."
2008-10-09 01:15:26.694 CHSVSR07 1504 1508 Sw_MessageHandler::Close - - - - 5 65535 "Shutdown complete."
2008-10-09 01:15:27.396 - 5192 5384 Sw_MessageHandler::Open - - - - 5 65535 "Initialization complete."
2008-10-09 01:15:28.673 CHSVSR07 5192 5384 Sw_SQLDataConnection::Open - - - - 2 41494 "Failed to establish a connection to the data source: (Server: CHSSQL01, Database: S
2008-10-09 01:15:28.673 CHSVSR07 5192 5384 Sw_SQLOutputHandler::Open - - - - 1 44910 "Failed to connect to data source."
2008-10-09 01:15:28.954 - 7432 6396 Sw_MessageHandler::Open - - - - 5 65535 "Initialization complete."
2008-10-09 01:15:29.016 - 6400 7732 Sw_MessageHandler::Open - - - - 5 65535 "Initialization complete."
2008-10-09 01:15:29.079 - 5732 6148 Sw_MessageHandler::Open - - - - 5 65535 "Initialization complete."
2008-10-09 01:15:29.904 CHSVSR07 6400 7732 Sw_SQLDataConnection::Open - - - - 2 41494 "Failed to establish a connection to the data source: (Server: CHSSQL01, Database: S
2008-10-09 01:15:29.904 CHSVSR07 6400 7732 Sw_SQLOutputHandler::Open - - - - 1 44910 "Failed to connect to data source."
2008-10-09 01:15:30.278 CHSVSR07 7432 6396 Sw_SQLDataConnection::Open - - - - 2 41494 "Failed to establish a connection to the data source: (Server: CHSSQL01, Database: S
2008-10-09 01:15:30.294 CHSVSR07 7432 6396 Sw_SQLOutputHandler::Open - - - - 1 44910 "Failed to connect to data source."
2008-10-09 01:15:30.356 CHSVSR07 5732 6148 Sw_SQLDataConnection::Open - - - - 2 41494 "Failed to establish a connection to the data source: (Server: CHSSQL01, Database: S
2008-10-09 01:15:30.356 CHSVSR07 5732 6148 Sw_SQLOutputHandler::Open - - - - 1 44910 "Failed to connect to data source."
2008-10-09 01:15:31.385 CHSVSR07 5192 5384 Sw_SystemDispatcher::Init - - - - 0 44951 "Successfully started Microsoft System Center Application Virtualization Management S
2008-10-09 01:15:36.785 CHSVSR07 7432 8120 Sw_LicenseConduitLogger::LogMessage 1956138080 "Default Provider" "Justin Zarb" TECHDES.001/TECHDES.001.sft 0 40976 "License Se
2008-10-09 01:15:36.941 CHSVSR07 7432 8120 Sw_RTSPHandler::HandleSetup 1956138080 "Default Provider" "Justin Zarb" TECHDES.001/TECHDES.001.sft 0 40960 "Session Setup"
2008-10-09 01:16:01.926 CHSVSR07 7432 5832 Sw_LicenseConduitLogger::LogMessage 1956138080 "Default Provider" "Justin Zarb" TECHDES.001/TECHDES.001.sft 0 40977 "License Se
2008-10-09 01:16:01.926 CHSVSR07 7432 5832 Sw_RTSPHandler::HandleTearDown 1956138080 "Default Provider" "Justin Zarb" TECHDES.001/TECHDES.001.sft 0 40961 "Session TearDown"
2008-10-09 01:20:32.766 CHSVSR07 6400 3444 Sw_LicenseConduitLogger::LogMessage 1897464568 "Default Provider" "Justin Zarb" SCVMCON.001/SCVMCON.001.sft 0 40976 "License
2008-10-09 01:20:32.766 CHSVSR07 6400 3444 Sw_RTSPHandler::HandleSetup 1897464568 "Default Provider" "Justin Zarb" SCVMCON.001/SCVMCON.001.sft 0 40960 "Session Setup"
2008-10-09 06:31:40.612 CHSVSR07 6400 8016 Sw_LicenseConduitLogger::LogMessage 1897464568 "Default Provider" "Justin Zarb" SCVMCON.001/SCVMCON.001.sft 0 40976 "License Abnormal
2008-10-09 06:31:40.663 CHSVSR07 6400 8016 Sw_SQLOutputHandler::HandleMessage - - - - 1 44911 "Create record failed with error [1]."
2008-10-09 06:35:40.367 CHSVSR07 5732 3960 Sw_DataConnectionPool::Reconnect - "Default Provider" "Justin Zarb" SCVMCON.001/SCVMCON.001.sft 2 41543 "Connection to data
2008-10-09 06:35:40.367 CHSVSR07 5732 3960 Sw_ServerAuthenticationTask::Authorize - "Default Provider" "Justin Zarb" SCVMCON.001/SCVMCON.001.sft 2 41472 "Module executi
2008-10-09 06:35:40.367 CHSVSR07 5732 5348 Sw_SQLOutputHandler::HandleMessage - - - - 1 44911 "Create record failed with error [1]."
2008-10-09 06:48:44.656 CHSVSR07 7432 6572 Sw_DataConnectionPool::Reconnect - "Default Provider" "Justin Zarb" SCVMCON.001/SCVMCON.001.sft 2 41543 "Connection to data store on host CHSSQL01\BQSTEPS faile
2008-10-09 06:48:44.656 CHSVSR07 7432 6572 Sw_ServerAuthenticationTask::Authorize - "Default Provider" "Justin Zarb" SCVMCON.001/SCVMCON.001.sft 2 41472 "Module execution failed."
2008-10-09 06:48:44.702 CHSVSR07 6400 3872 Sw_DataConnectionPool::Reconnect - "Default Provider" "Justin Zarb" SCVMCON.001/SCVMCON.001.sft 2 41543 "Connection to data store on host CHSSQL01\BQSTEPS faile
2008-10-09 06:48:44.702 CHSVSR07 7432 7864 Sw_SQLOutputHandler::HandleMessage - - - - 1 44911 "Create record failed with error [1]."
2008-10-09 06:48:44.702 CHSVSR07 6400 5872 Sw_ServerAuthenticationTask::Authorize - "Default Provider" "Justin Zarb" SCVMCON.001/SCVMCON.001.sft 2 41472 "Module execution failed."
2008-10-09 08:33:07.803 CHSVSR07 5732 6508 Sw_LicenseConduitLogger::LogMessage 231148567 "Default Provider" Swelshman SIMSNET.005/SIMSNET.005.sft 0 40976 "License Sessi
2008-10-09 08:33:07.818 CHSVSR07 5732 6508 Sw_RTSPHandler::HandleSetup 231148567 "Default Provider" Swelshman SIMSNET.005/SIMSNET.005.sft 0 40960 "Session Setup"
2008-10-09 08:39:02.202 CHSVSR07 5732 3960 Sw_LicenseConduitLogger::LogMessage 2076584603 "Default Provider" YMSWOOD SIMSNET.005/SIMSNET.005.sft 0 40976 "License Sessi
2008-10-09 08:39:02.218 CHSVSR07 5732 3960 Sw_RTSPHandler::HandleSetup 2076584603 "Default Provider" YMSWOOD SIMSNET.005/SIMSNET.005.sft 0 40960 "Session Setup"
2008-10-09 08:44:58.679 CHSVSR07 7432 6492 Sw_LicenseConduitLogger::LogMessage 1008015806 "Default Provider" DLANEY ADDR811.001/ADDR811.001.sft 0 40976 "License Session
2008-10-09 08:44:58.726 CHSVSR07 7432 6492 Sw_RTSPHandler::HandleSetup 1008015806 "Default Provider" DLANEY ADDR811.001/ADDR811.001.sft 0 40960 "Session Setup"
2008-10-09 08:45:01.412 CHSVSR07 7432 1528 Sw_LicenseConduitLogger::LogMessage 1008015806 "Default Provider" DLANEY ADDR811.001/ADDR811.001.sft 0 40977 "License Session

```

Hacker 最常做的就是



相關網站

- Exploit DB
 - <http://www.exploit-db.com/>
- CVE
 - <http://cve.mitre.org/>
- 1337 Day
 - <http://1337day.com/>
- Packetstorm
 - <http://packetstormsecurity.com/>
- SCAP
 - <http://www.scap.org.cn/>
- Zone-h
 - <http://www.zone-h.org/>



滲透測試環境



NEXUS 10 TABLET

NEXUS 7 MINI-TABLET

NEXUS 5 MOBILE PHONE

建立滲透測試環境

- Update Kali
- Install Chrome
- 跳板
- 帳號/密碼
 - root/toor



Update Kali

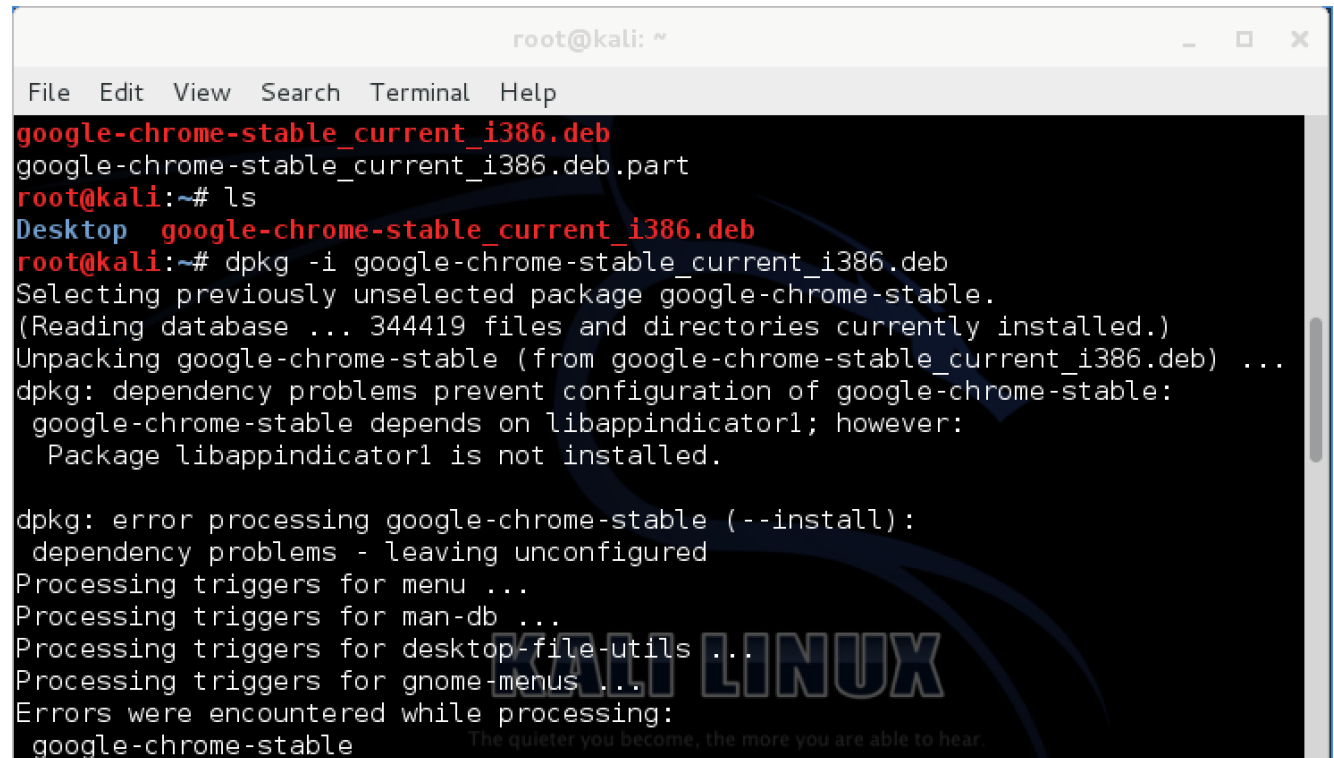
- 更新Kali 以確保本身的狀態是最新的
 - \$ apt-get update
 - \$ apt-get upgrade

GoogleChrome



```
dpkg -i google-chrome-stable_current_i386.deb
```

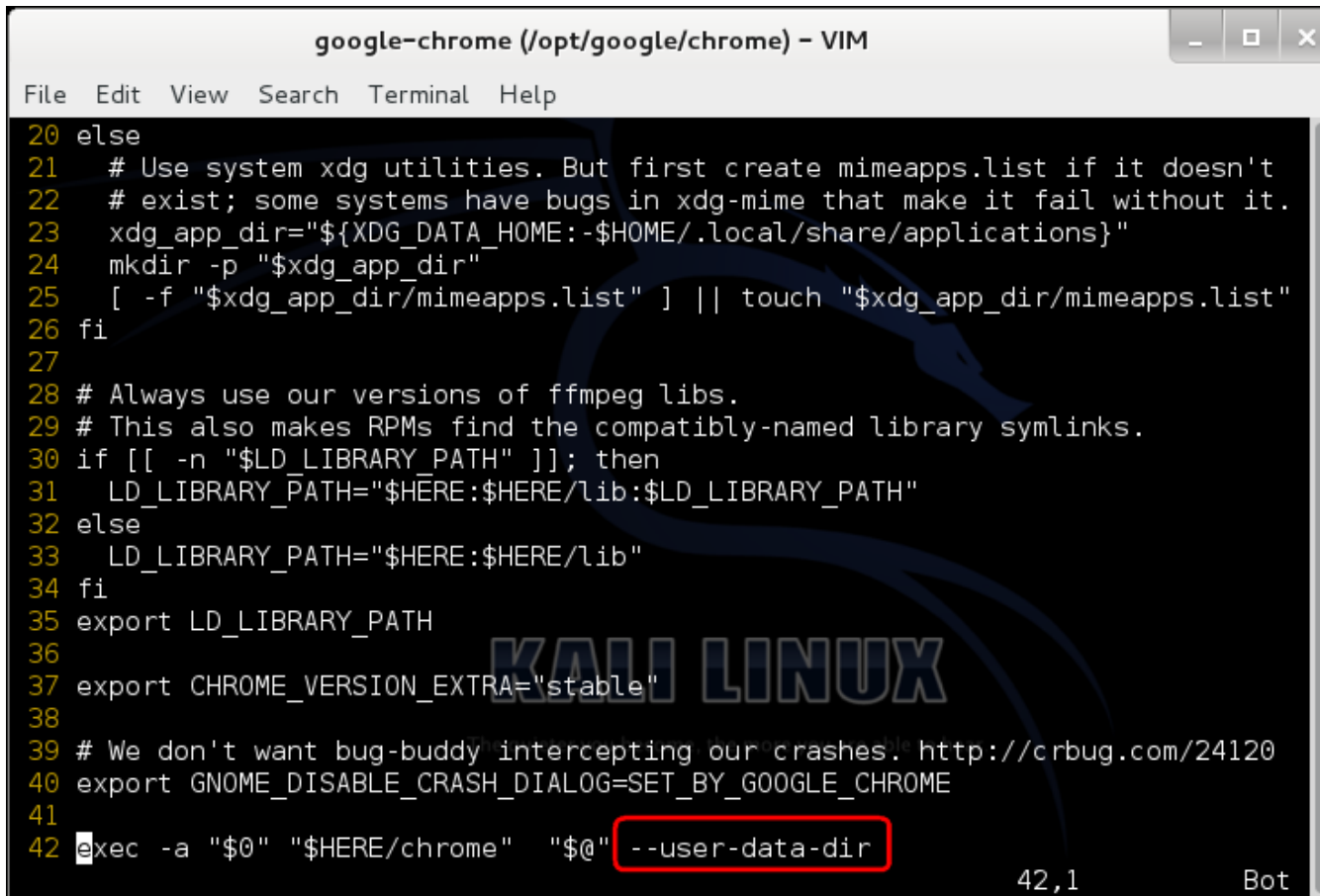

- 如果安裝上有問題的話
 - apt-get install -f
 - dpkg -i google-chrome-stable_current_i386.deb



```
root@kali: ~  
File Edit View Search Terminal Help  
google-chrome-stable_current_i386.deb  
google-chrome-stable_current_i386.deb.part  
root@kali:~# ls  
Desktop google-chrome-stable_current_i386.deb  
root@kali:~# dpkg -i google-chrome-stable_current_i386.deb  
Selecting previously unselected package google-chrome-stable.  
(Reading database ... 344419 files and directories currently installed.)  
Unpacking google-chrome-stable (from google-chrome-stable_current_i386.deb) ...  
dpkg: dependency problems prevent configuration of google-chrome-stable:  
 google-chrome-stable depends on libappindicator1; however:  
  Package libappindicator1 is not installed.  
  
dpkg: error processing google-chrome-stable (--install):  
 dependency problems - leaving unconfigured  
Processing triggers for menu ...  
Processing triggers for man-db ...  
Processing triggers for desktop-file-utils ...  
Processing triggers for gnome-menus ...  
Errors were encountered while processing:  
 google-chrome-stable
```

GoogleChrome

- vim /opt/google/chrome/google-chrome



```
google-chrome (/opt/google/chrome) - VIM
File Edit View Search Terminal Help
20 else
21 # Use system xdg utilities. But first create mimeapps.list if it doesn't
22 # exist; some systems have bugs in xdg-mime that make it fail without it.
23 xdg_app_dir="${XDG_DATA_HOME:-$HOME/.local/share/applications}"
24 mkdir -p "$xdg_app_dir"
25 [ -f "$xdg_app_dir/mimeapps.list" ] || touch "$xdg_app_dir/mimeapps.list"
26 fi
27
28 # Always use our versions of ffmpeg libs.
29 # This also makes RPMs find the compatibly-named library symlinks.
30 if [[ -n "$LD_LIBRARY_PATH" ]]; then
31 LD_LIBRARY_PATH="$HERE:$HERE/lib:$LD_LIBRARY_PATH"
32 else
33 LD_LIBRARY_PATH="$HERE:$HERE/lib"
34 fi
35 export LD_LIBRARY_PATH
36
37 export CHROME_VERSION_EXTRA="stable"
38
39 # We don't want bug-buddy intercepting our crashes. http://crbug.com/24120
40 export GNOME_DISABLE_CRASH_DIALOG=SET_BY_GOOGLE_CHROME
41
42 exec -a "$0" "$HERE/chrome" "$@" --user-data-dir
42,1 Bot
```

VPN 連線

- 新增VPN連線
 - apt-get install network-manager-openvpn-gnome
 - apt-get install network-manager-pptp
 - apt-get install network-manager-pptp-gnome
 - apt-get install network-manager-strongswan
 - apt-get install network-manager-vpnc
 - apt-get install network-manager-vpnc-gnome
 - /etc/init.d/network-manager restart

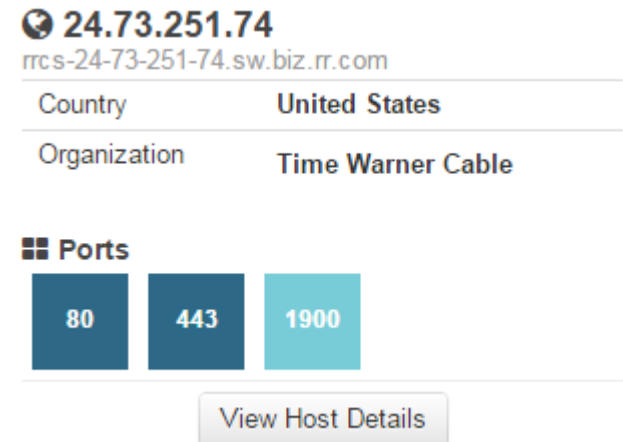
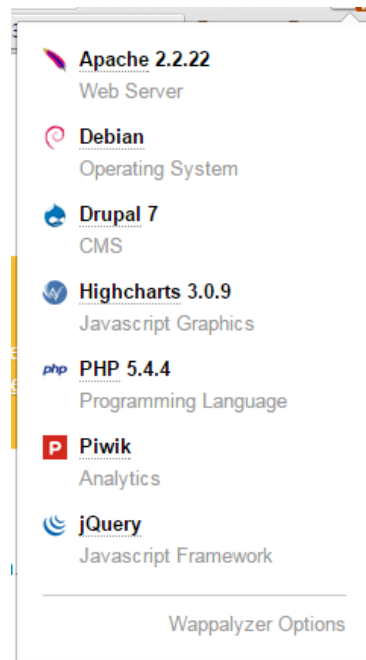
資訊蒐集

- 資訊蒐集為滲透測試之首要工作，收集的內容包含：
 - 網路架構
 - DNS資訊
 - 主機資訊
 - Email帳號
 - SNMP資訊
 - 通訊錄
 - 文件檔
 - 其他



關於瀏覽器的套件

- wappalyzer小工具有助於了解一個網站所使用的系統，例如:作業系統版本、所使用的程式語言、以及這個網站有用什麼樣的套件等
- Shodan 可以很快地告訴你現在目前網站的IP、所屬位址、甚至可以告訴你目前這台伺服器開的服務，以及伺服器所使用的套件。



關於瀏覽器的套件

- ip-address-and-domain
小工具有助於了解網域相關資訊
- PortScan可以幫助你檢測
對目標主機進行服務的掃描

TCIPUTILS.com

8+1 1,114

Home -> IPv4 root -> 173/8 -> 173.194.112.0/24 -> 173.194.112.1

type domain, IPv4/IPv6 or provider

IP information 173.194.112.1

IP address	173.194.112.1
Description	Google Inc.
Location	Mountain View, California, United States (US)
Registry	arin

Network information

IP address	173.194.112.1
Reverse DNS (PTR record)	fra07s27-in-f1.1e100.net
DNS server (NS record)	ns1.google.com (216.239.32.10) ns4.google.com (216.239.38.10) ns3.google.com (216.239.36.10) ns2.google.com (216.239.34.10)
ASN number	15169
ASN name (ISP)	Google Inc.
IP-range/subnet	173.194.112.0/24 173.194.112.0 - 173.194.112.255

[Ping 173.194.112.1](#)

URL/Domain Name/IP Address:

Start port: End port:

Enter port numbers separated by space. (e.g. 21 25 80)

These are common ports used by most of Trojan.

Developed with ♥ in India by [Abhijeet Ashok Muneshwar](#)

資訊收集

- Google hacking
- 主機資訊收集
 - Maltego
- Dns 資訊收集
 - Dnsmap
 - Dnswalk

GoogleHacking

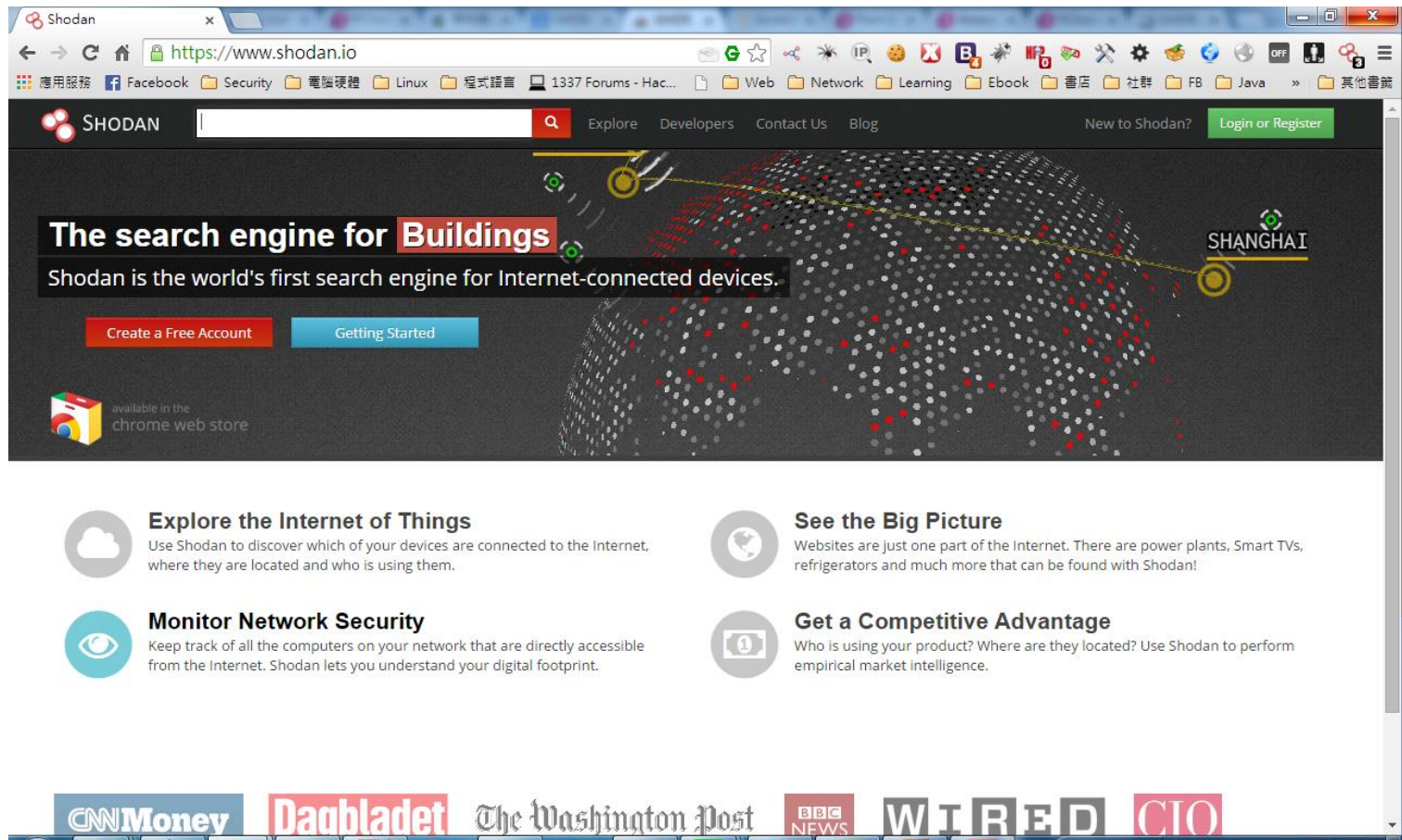
- site: (.edu, .gov, honeynet.org.tw)
- filetype: (txt, xls, mdb, pdf, .log)
- Intitle / allintitle
- Inurl / allinurl

GHDB with Chrome

- Google Hack Data Base - application to work with GHDB. Choose a category and click on the necessary query.



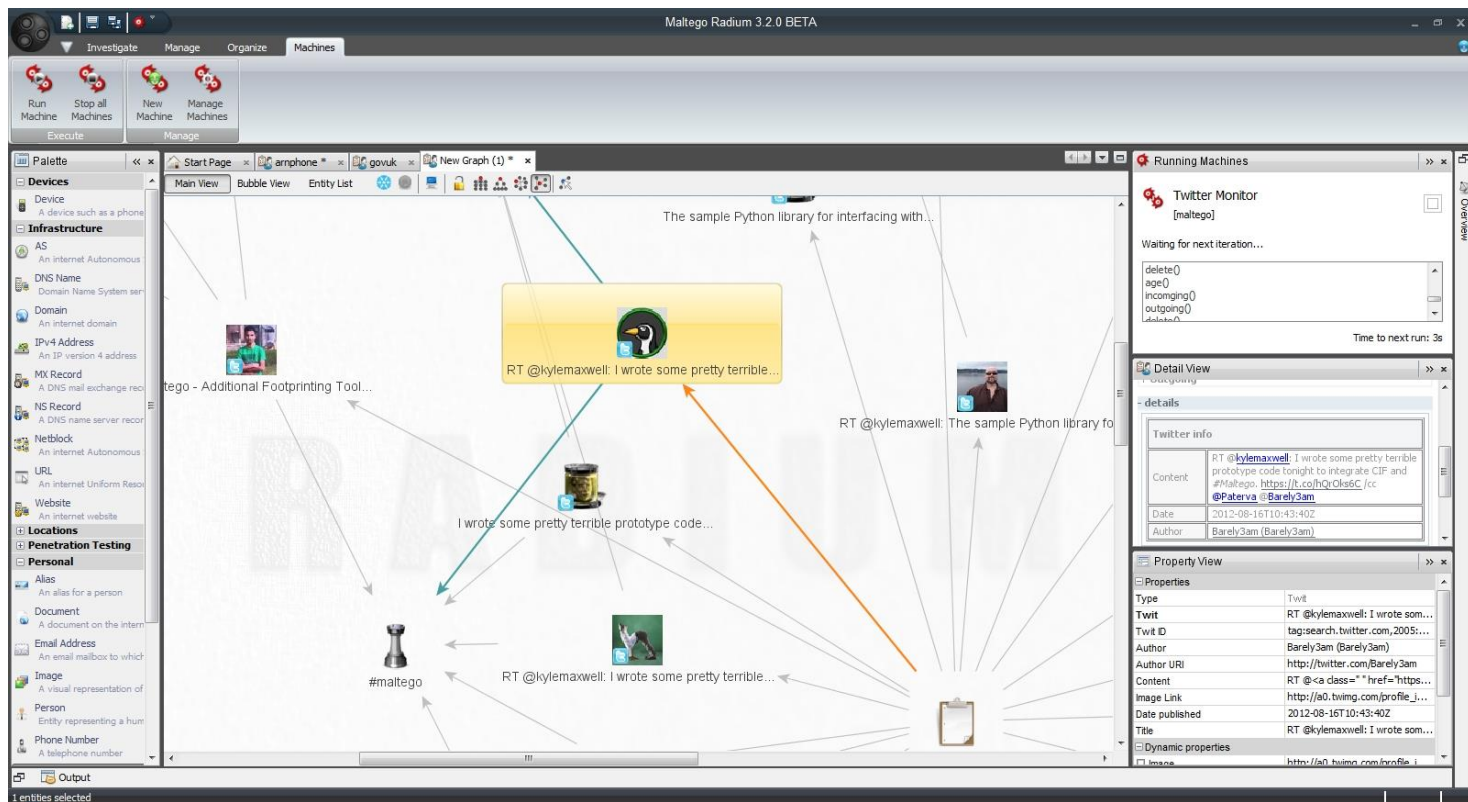
SHODAN



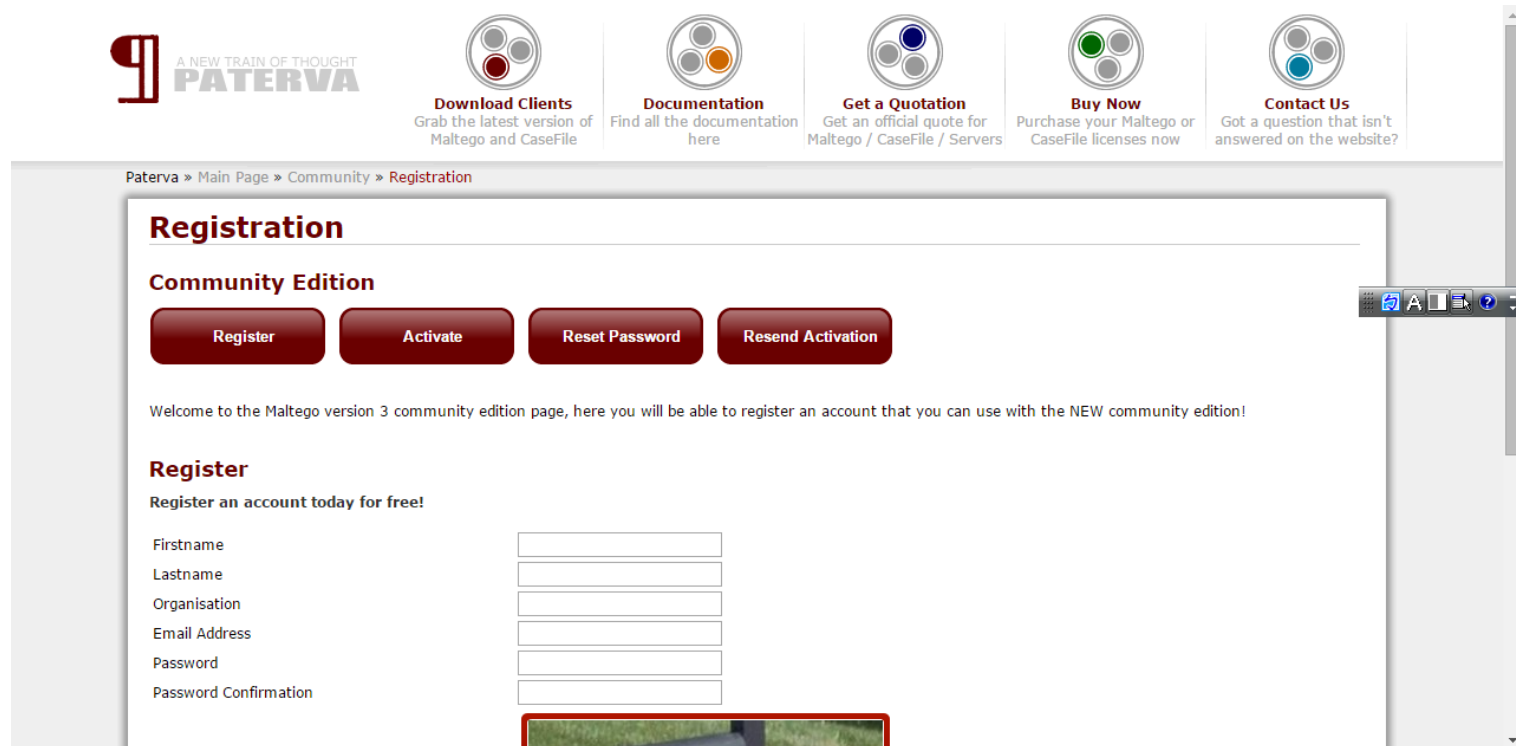
<https://www.shodan.io/>

Maltego

- Maltego 是一套網路情報與偵察應用工具，可以清楚呈現網路環境中的威脅關係圖像之平台。它可以將一個網路架構中的單個實體的所有關係完整的表現出來。



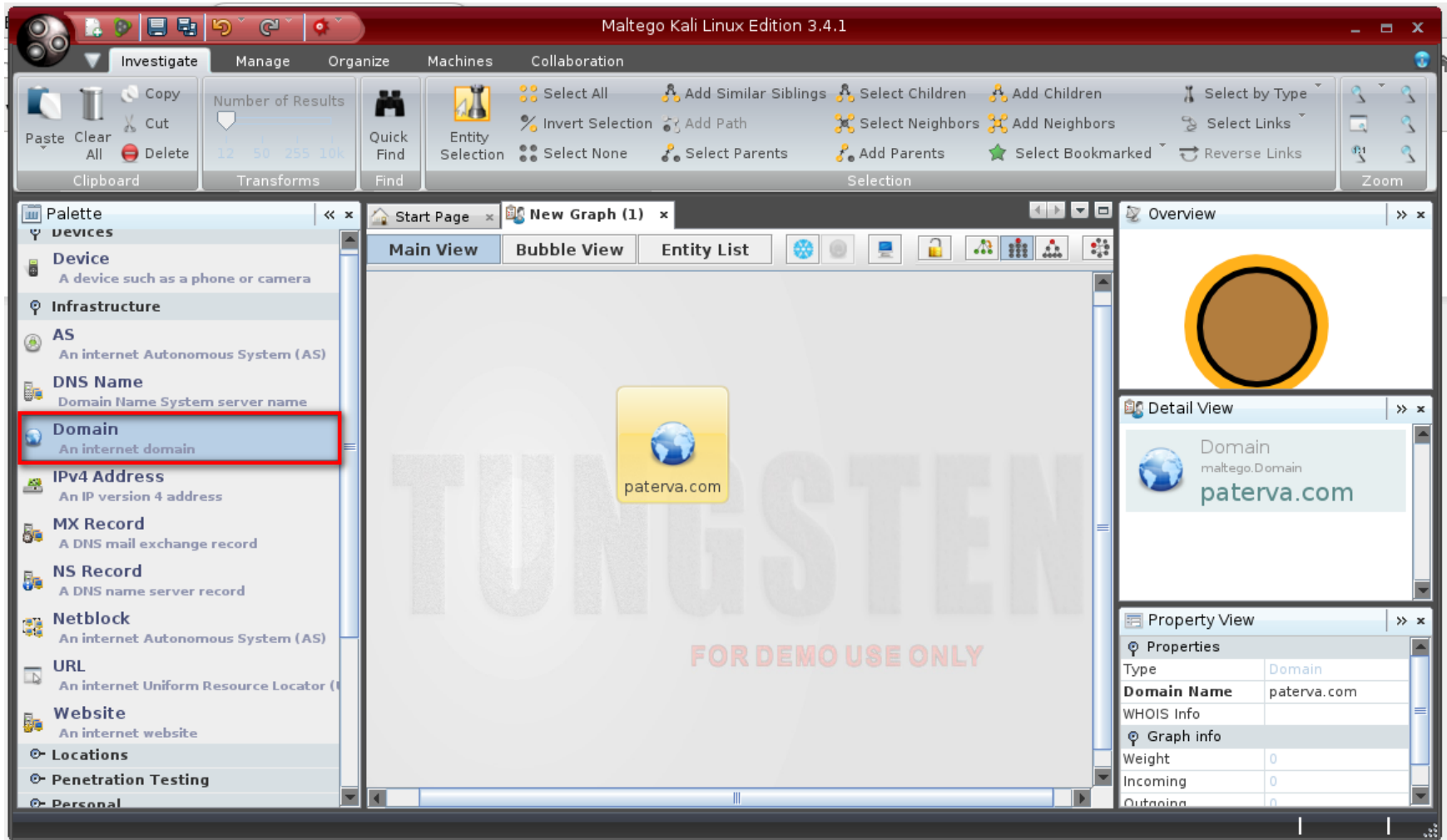
先註冊一個帳號



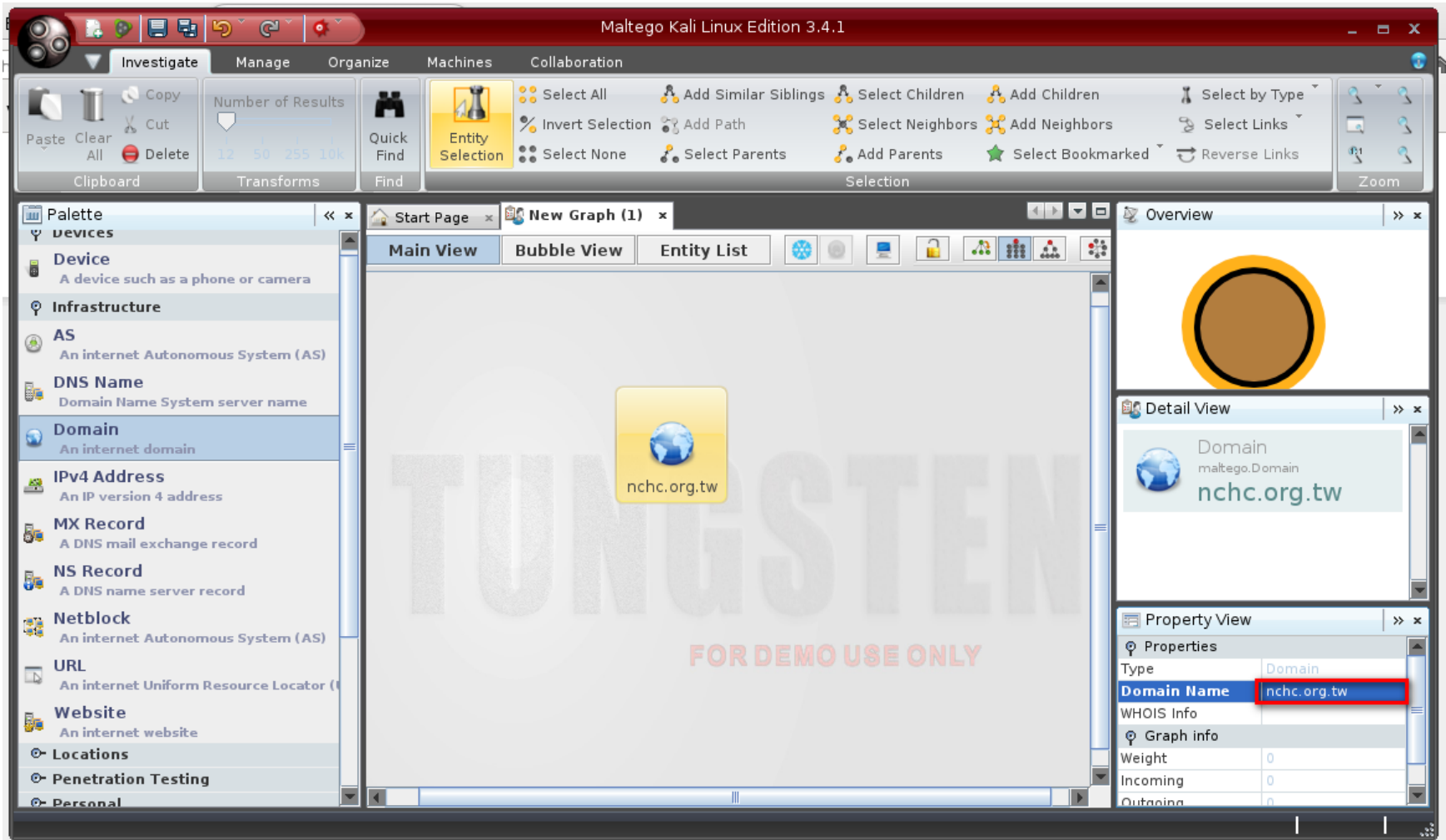
The screenshot shows the Paterva website's registration page. At the top, there is a navigation bar with the Paterva logo and several links: Download Clients, Documentation, Get a Quotation, Buy Now, and Contact Us. Below this, the breadcrumb trail reads: Paterva » Main Page » Community » Registration. The main heading is "Registration" followed by "Community Edition". There are four buttons: Register, Activate, Reset Password, and Resend Activation. A welcome message states: "Welcome to the Maltego version 3 community edition page, here you will be able to register an account that you can use with the NEW community edition!". The "Register" section includes the prompt "Register an account today for free!" and a form with fields for Firstname, Lastname, Organisation, Email Address, Password, and Password Confirmation. A small image of a train is visible at the bottom of the form.

- <https://www.paterva.com/web6/community/maltego/>

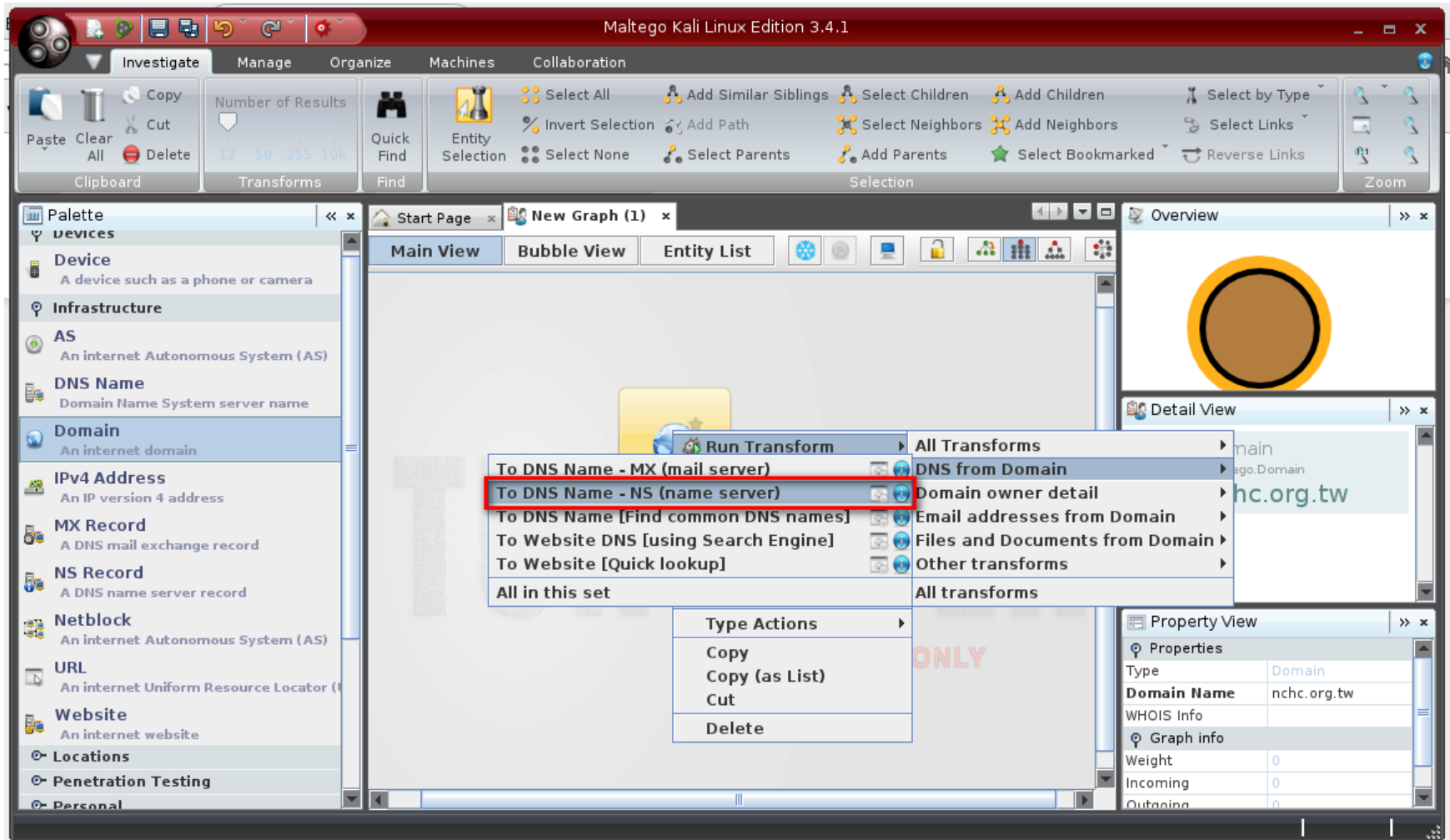
Maltego



Maltego



Maltego



Maltego

The screenshot displays the Maltego Kali Linux Edition 3.4.1 interface. The main window shows a graph titled "New Graph (1)" with a central entity "nchc.org.tw" (represented by a globe icon) connected to two child entities, "ns1.nchc.org.tw" and "ns2.nchc.org.tw" (represented by server icons). The interface includes a top menu bar with "Investigate", "Manage", "Organize", "Machines", and "Collaboration". Below the menu is a toolbar with various icons for clipboard, transforms, find, and selection. The left sidebar contains a "Palette" with categories like "Devices", "Infrastructure", "AS", "DNS Name", "Domain", "IPv4 Address", "MX Record", "NS Record", "Netblock", "URL", "Website", "Locations", "Penetration Testing", and "Personal". The right sidebar has three panels: "Overview" showing a small graph, "Detail View" showing the "Domain" properties for "nchc.org.tw", and "Property View" showing a table of properties.

Overview

Detail View

Domain
maltego.Domain
nchc.org.tw

+ Relationships

Property View

Properties	
Type	Domain
Domain Name	nchc.org.tw
WHOIS Info	
Graph info	
Weight	0
Incoming	0
Outgoing	3

Output - Transform Output

Running transform To DNS Name - NS (name server) on 1 entities.
Transform To DNS Name - NS (name server) returned with 3 entities.
Transform To DNS Name - NS (name server) done

DNS紀錄的類型

- DNS record
 - NS(name server):網域名稱
 - A(address):網域名稱所對應的IPv4位址
 - AAAA(address):網域名稱所對應的IPv6位址
 - MX(mail exchanger)：郵件伺服器
 - PTR(pointer):反解資訊

DNS資訊蒐集

- 網路公開資訊查詢
 - <http://www.whois365.com/tw/>

全球 WHOIS 查詢[關於 Whois365.com](#)[gTLD & ccTLD 列表](#)[工具](#)[English](#)[简体中文](#)

請輸入網域名稱或 IP 位址 [說明](#)

請輸入要查詢的網域名稱 (不包含 "http://" URI 或 "www." 次網域) 或 IP 位址，然後按 "進行查詢" 繼續。

支援 IDN (國際化網域名稱) 網域查詢

© 2006-2009 全球 WHOIS 查詢 [網站地圖](#) [搜尋 Whois365.com](#) [加入書籤](#) Top

IP 位址 : 58.63.238.212

PTR : --

註冊局 WHOIS 主機 : whois.apnic.net:43

% [whois.apnic.net]

% Whois data copyright terms <http://www.apnic.net/db/dbcopyright.html>

% Information related to '58.60.0.0 - 58.63.255.255'

inetnum: 58.60.0.0 - 58.63.255.255

netname: CHINANET-GD

descr: CHINANET Guangdong province network

descr: China Telecom

descr: No.31 jingrong street

descr: Beijing 100032

country: CN

admin-c: CH93-AP

tech-c: IC83-AP

mnt-by: APNIC-HM

mnt-lower: MAINT-CHINANET-GD

mnt-routes: MAINT-CHINANET-GD

status: ALLOCATED PORTABLE

remarks: ++++++This object can only be updated by APNIC hostmasters.

remarks: To update this object, please contact APNIC

remarks: hostmasters and include your organisation's account

remarks: name in the subject line.

remarks: ++++++

changed: hm-changed (at) apnic.net 20050816

source: APNIC

person: Chinanet Hostmaster

nic-hdl: CH93-AP

e-mail: anti-spam (at) ns.chinanet.cn.net

address: No.31 jingrong street,beijing

address: 100032

phone: +86-10-58501724

fax-no: +86-10-58501724

country: CN

changed: dingsy (at) cndata.com 20070416

mnt-by: MAINT-CHINANET

source: APNIC

person: IPMASTER CHINANET-GD

nic-hdl: IC83-AP

e-mail: ipadm (at) 189.cn

address: NO.1,RO DONGYUANHENG,YUEXIUNAN,GUANGZHOU

phone: +86-20-83877223

fax-no: +86-20-83877223

country: CN

changed: ipadm (at) 189.cn 20110418

mnt-by: MAINT-CHINANET-GD

remarks: IPMASTER is not for spam complaint,please send spam complaint to abuse_gdnoc (at) 189.cn

abuse-mailbox: abuse_gdnoc (at) 189.cn

source: APNIC

% This query was served by the APNIC Whois Service version 1.68 (WHOIS3)

關於 Dns Zone transfer



資安人
INFO SECURITY
作對事、用對方法、找對夥伴

台北場: 10月23日(四) 新竹場: 10月24日(五)
特別演講貴賓
勤業眾信/資訊長暨風險管理顧問總經理/萬幼筠 **免費報名**

加入會員 · 會員登入

請輸入您要查詢的關鍵字

[首頁](#) |
 [焦點新聞](#) |
 [資安知識庫](#) |
 [研討會](#) |
 [產業快訊](#) |
 [個資法專區](#) |
 [資安急診室](#) |
 [資安免費工具](#) |
 [VIP](#) |
 [\[免費報名\]](#)

首頁 > 焦點新聞

透過DNS區域轉送攻擊 政府、電信主機資訊被看光光

作者: 張維君 - 05/12/2014



駭客在入侵企業系統前，必定會以各種刺探方式掌握目標對象的主機、IP位址、設備等資訊，再搭配系統弱點就可以長驅直入。早在15年前就被提出的DNS區域轉送攻擊(Zone Transfer)，正是可被用來取得組織內部伺服器資訊的手法，目前全台卻仍有包括台北市政府在內的政府機關、知名電信業者、電子商務、人力銀行等網站有此漏洞，其系統正暴露在高度風險之中。

資安廠商DEVCORE在進行網路監控時發現此一問題，在Alexa TW Top 525當中有48個網域仍存有Zone Transfer漏洞。DEVCORE執行長翁浩正表示，透過此一漏洞，即可讓駭客掌握目標對象的內網配置，包括有哪些主機、主機IP位址或設備等資訊，只要再搭配未修補的系統弱點，很容易就被取得控制權限。

翁浩正進一步指出，此一漏洞屬於網管設定的問題，在Windows系統只要到伺服器管理

「謹守智財 延續企業競爭力」研討會

觀念對了、方法對了
就可將有限資源極大化應用

台北場: 10月23日(四)
新竹場: 10月24日(五)

免費報名

本週新聞點閱排行

內賊難防！建立及早發現與完善稽核防護機制

勇奪2014全球駭客大賽亞軍 台灣駭客團隊 HITCON

Hacktivism發酵 駭客更愛竊取大企業的資料

無需過度恐慌，但別掉以輕心: Shellshock

NASA又傳員工筆電遭竊 至少萬筆個資外洩

DDoS攻擊手法與防禦對策-DDoS網災來襲 政府準備好了嗎？<攻防技術篇之二>

http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=7846

關於 Dns Zone transfer 檢測

- Linux 檢測
 - dig +nostats +nocomments +nocmd NS zonetransfer.me
 - dig axfr zonetransfer.me @ns12.zoneedit.com
- Windows 檢測
 - nslookup -type=ns zonetransfer.me
 - nslookup
server ns12.zoneedit.com
ls -d zonetransfer.me

```
C:\Users\chingshiung>nslookup -type=ns zonetransfer.me
伺服器: UnKnown
Address: 172.20.10.1

未經授權的回答:
zonetransfer.me nameserver = nsztm1.digi.ninja
zonetransfer.me nameserver = nsztm2.digi.ninja
```

<http://digi.ninja/projects/zonetransferme.php>

關於 Dns Zone transfer 檢測

```

C:\Users\chingshiung>nslookup
預設伺服器: UnKnown
Address: 172.20.10.1

> server nsztml.digi.ninja
預設伺服器: nsztml.digi.ninja
Address: 167.88.42.94

> ls -d zonetransfer.me
[nsztml.digi.ninja]
zonetransfer.me.      SOA      nsztml.digi.ninja robin.digi.ninja. (2014
101501 172800 900 1209600 3600)
zonetransfer.me.      TXT      "google-site-verification=tyP28J
7JAUHA9fw2sHXMgcCC0I6XBmmoUi04UIMewxA"

zonetransfer.me.      MX       0        ASPMX.L.GOOGLE.COM
zonetransfer.me.      MX       10       ALT1.ASPMX.L.GOOGLE.COM
zonetransfer.me.      MX       10       ALT2.ASPMX.L.GOOGLE.COM
zonetransfer.me.      MX       20       ASPMX2.GOOGLEMAIL.COM
zonetransfer.me.      MX       20       ASPMX3.GOOGLEMAIL.COM
zonetransfer.me.      MX       20       ASPMX4.GOOGLEMAIL.COM
zonetransfer.me.      MX       20       ASPMX5.GOOGLEMAIL.COM
zonetransfer.me.      A        217.147.180.162
zonetransfer.me.      NS       nsztml.digi.ninja
zonetransfer.me.      NS       nsztml2.digi.ninja
_sip._tcp
transfer.me           SRU      priority=0, weight=0, port=5060, www.zone
transfer.me
164.180.147.217.IN-ADDR.ARPA PTR      www.zonetransfer.me
asfdbauthdns         AFSDB    1        asfdbbox.zonetransfer.me
asfdbbox              A        127.0.0.1
asfdbvolume           AFSDB    1        asfdbbox.zonetransfer.me
canberra-office      A        202.14.81.230

```

dnsmap

- Dnsmap 是一個專門收集 subdomain 資訊的工具。
- Example:
 - dnsmap naver.com

```
root@kaliX201:~# dnsmap naver.com -r ./dns_naver_results.txt
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] searching (sub)domains for naver.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

ad.naver.com
IP address #1: 103.6.174.8
IP address #2: 103.6.174.7

ax.naver.com
IP address #1: 111.91.132.22

beta.naver.com
IP address #1: 112.175.153.78
```

<https://code.google.com/p/dnsmap/>

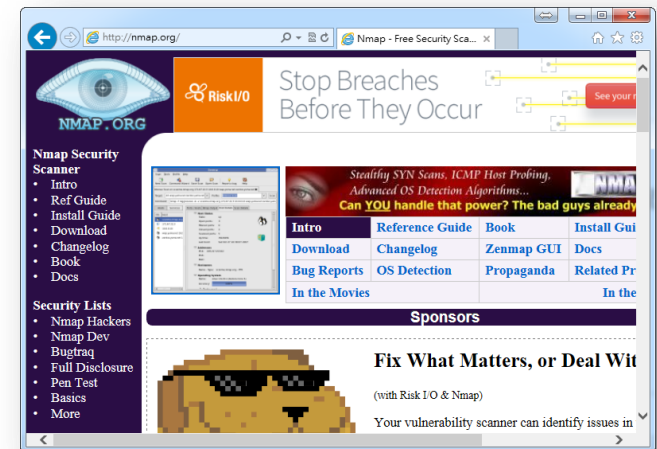
dnswalk

- dnswalk是一個可以測試你的dns 是否有zone transfer 的小工具。
- Example:
 - dnswalk abc.om.

```
root@kaliX201:~# dnswalk
defined(@array) is deprecated at /usr/bin/dnswalk line 61.
(Maybe you should just omit the defined()?)
Usage: dnswalk domain
domain MUST end with a '.'
root@kaliX201:~# dnswalk ocu.edu.tw.
defined(@array) is deprecated at /usr/bin/dnswalk line 61.
(Maybe you should just omit the defined()?)
Checking ocu.edu.tw.
Getting zone transfer of ocu.edu.tw. from ns01.ocu.edu.tw...done.
SOA=ns01.ocu.edu.tw      contact=root.rs2.ocu.edu.tw
BAD: bi.ocu.edu.tw NS dns.bi.ocu.edu.tw: unknown host
WARN: cloud-01.ocu.edu.tw A 10.8.11.1: no PTR record
WARN: cloud-02.ocu.edu.tw A 10.8.11.2: no PTR record
WARN: cloud-03.ocu.edu.tw A 10.8.11.3: no PTR record
```

網路與主機掃描-Nmap

- Nmap是由Fyodor Vaskovich所開發的一套開放原始碼軟體
- Nmap主要用於針對本機或遠端主機進行網路連接埠、應用程式類別、作業系統版本...等電腦資訊。
- Zenmap是nmap的圖形化介面版本

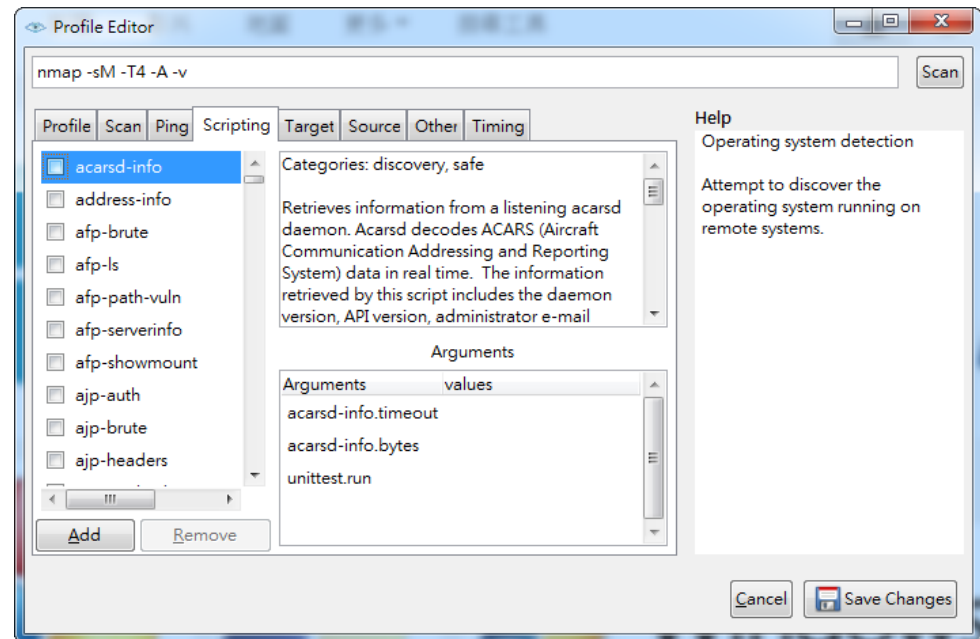


網路與主機掃描-Nmap

- 指令介紹：
 - sT 掃描已建立的TCP 連線
 - sS 掃描標示為SYN的TCP封包
 - sA 透過Ping的方式進行掃描
 - P 指定連接埠的掃描範圍
 - A 顯示操作系統與應用程式版本 (-Sv -O)
 - v 顯示詳細資訊

Nmap NSE Script

- Nmap的腳本引擎，是目前Nmap的最強大的特色，藉由執行這些腳本可以完成各種各樣的自動化任務。
- 使用者本身也可以撰寫自己所需要的腳本，來滿足任務的需求。



網路與主機掃描-Nmap

- nmap -A 127.0.0.1

```
root@kali:~# nmap -A 192.168.195.134

Starting Nmap 6.40 ( http://nmap.org ) at 2013-11-15 14:56 CST
Nmap scan report for 192.168.195.134
Host is up (0.00033s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey: 1024 60:0f:cf:el:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN,
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OC0SA/s
|_Not valid before: 2010-03-17T14:07:45+00:00
|_Not valid after: 2010-04-16T14:07:45+00:00
|_ssl-date: 2013-11-15T06:54:18+00:00; -2m49s from local time.
53/tcp    open  domain       ISC BIND 9.4.2
|_dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind      2 (RPC #100000)
|_rpcinfo:
|_program version  port/proto  service
|_100000 2 111/tcp    rpcbind
|_100000 2 111/udp    rpcbind
|_100003 2,3,4 2049/tcp   nfs
|_100003 2,3,4 2049/udp   nfs
|_100005 1,2,3 33418/udp  mountd
|_100005 1,2,3 47871/tcp  mountd
|_100021 1,3,4 32883/udp  nlockmgr
|_100021 1,3,4 37465/tcp  nlockmgr
```

TCP Connect /Full | Half Open Scan



SYN Packet+ Port(n)



SYN/ACK Packet



ACK + RST



SYN Packet+ Port80



SYN/ACK Packet



RST



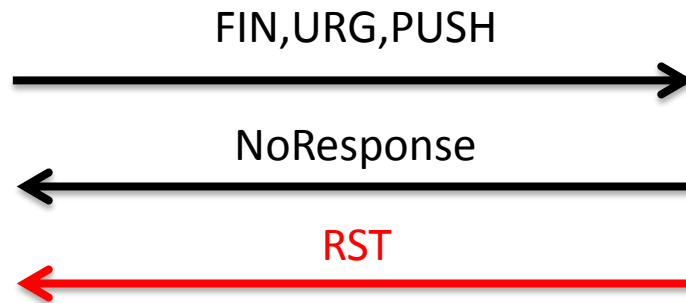
SYN Packet+ Port 80



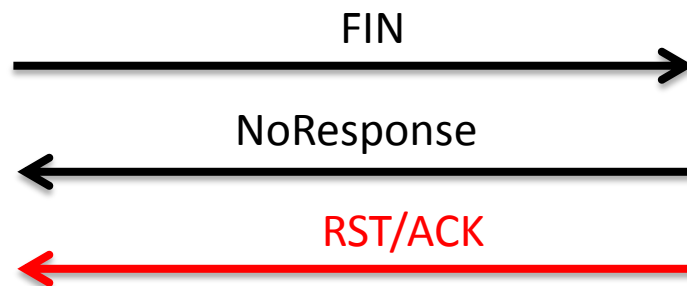
RST



Xmas / Fin Scan

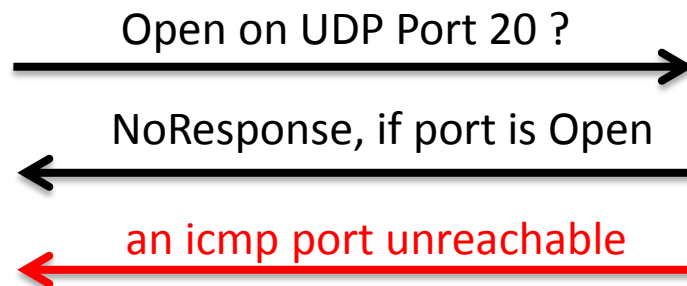
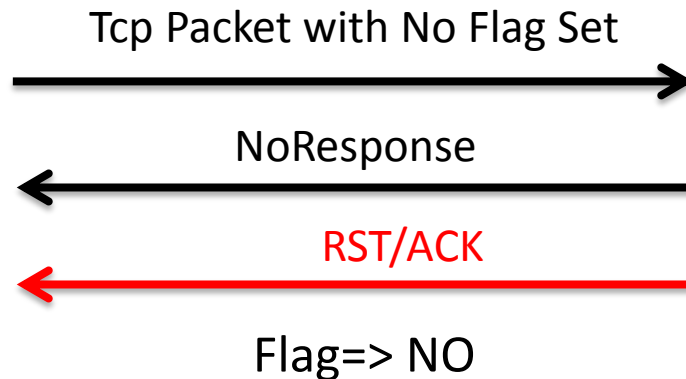


Flag=>URG,ACK,RST,SYN,FIN



Flag=>FIN

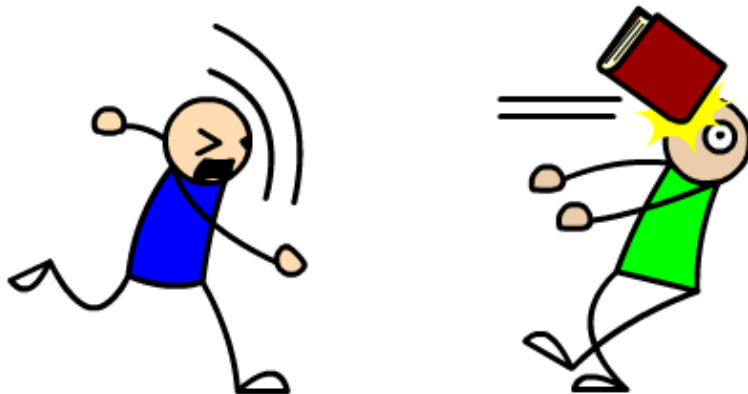
Null / UDP Scan



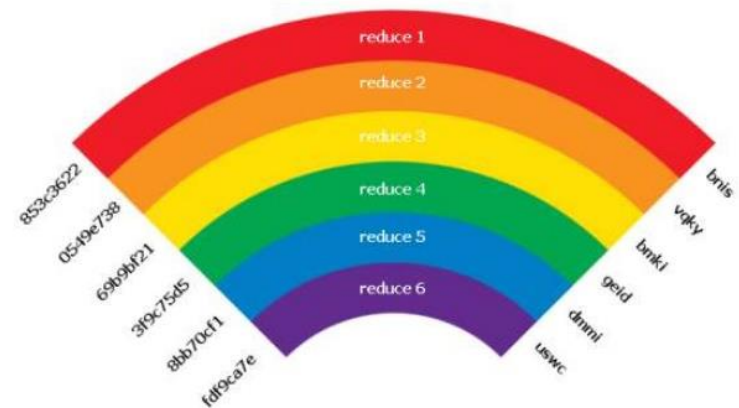
密碼破解



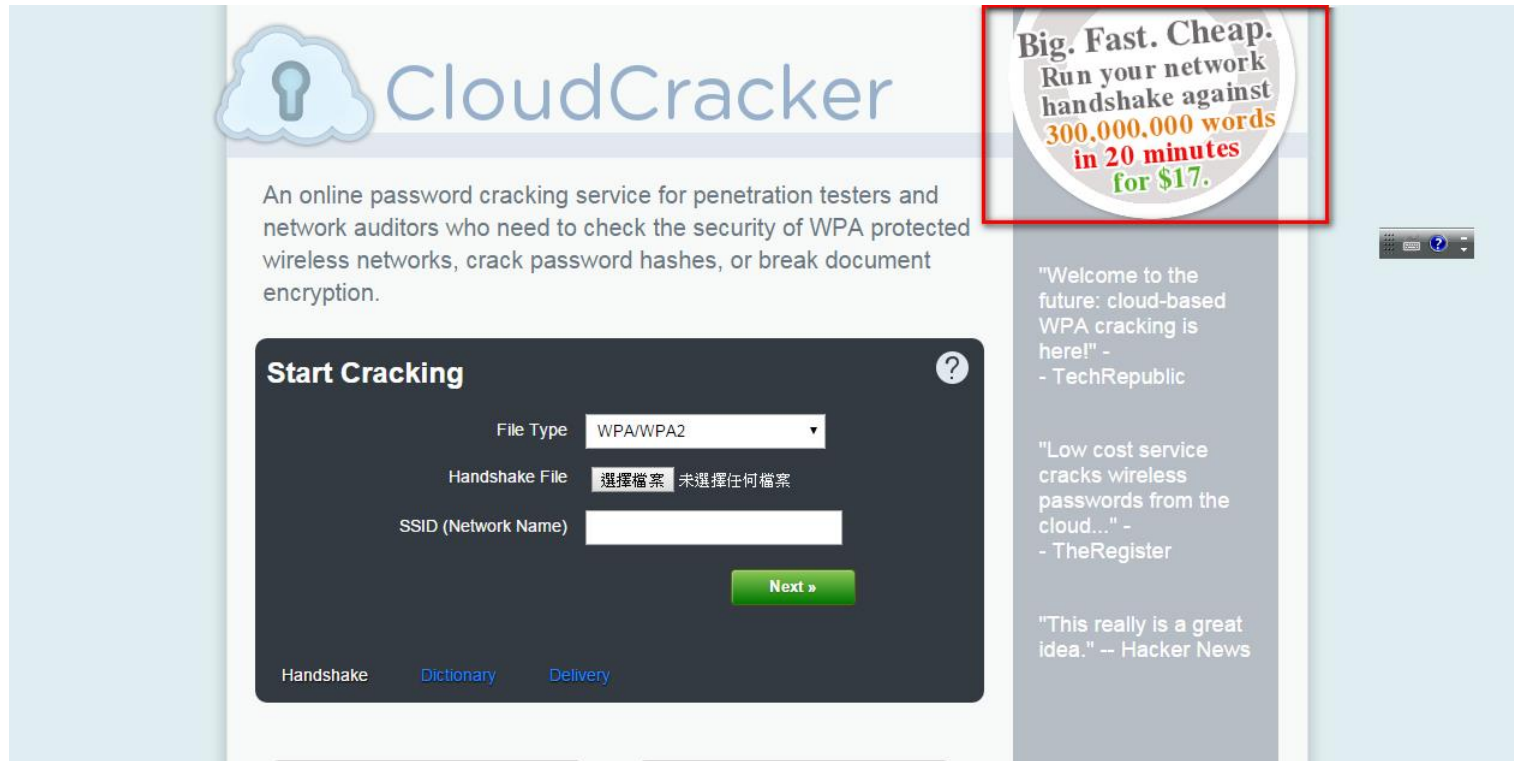
DICTIONARY ATTACK!



What is a Rainbow Table ?



當密碼上雲端



<https://www.cloudcracker.com/>

密碼與Gpu的火花

- Hashcat 一款可以支援Gpu運算來進行密碼的破解，本身可以運行在Windows與Linux 平台，必需搭配特定版本的顯示卡驅動程式，才可運行軟體。



hashcat
advanced
password
recovery

hash-identifier

- 為blackploit 所開發維護，如同本身的名字一樣hash-identifier 可以幫助你快速了解，你所輸入的字串的加密類型。
- Encryption formats supported:
 - ADLER-32
 - CRC-32
 - CRC-32B
 - CRC-16
 - CRC-16-CCITT
 - DES(Unix)
 - FCS-16
 -



hash-identifier

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# hash-identifier  
#####  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#####  
  
-----  
HASH: e10adc3949ba59abbe56e057f20f883e  
  
Possible Hashes:  
[+] MD5  
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))  
  
Least Possible Hashes:  
[+] RAdmin v2.x  
[+] NTLM
```

密碼破解

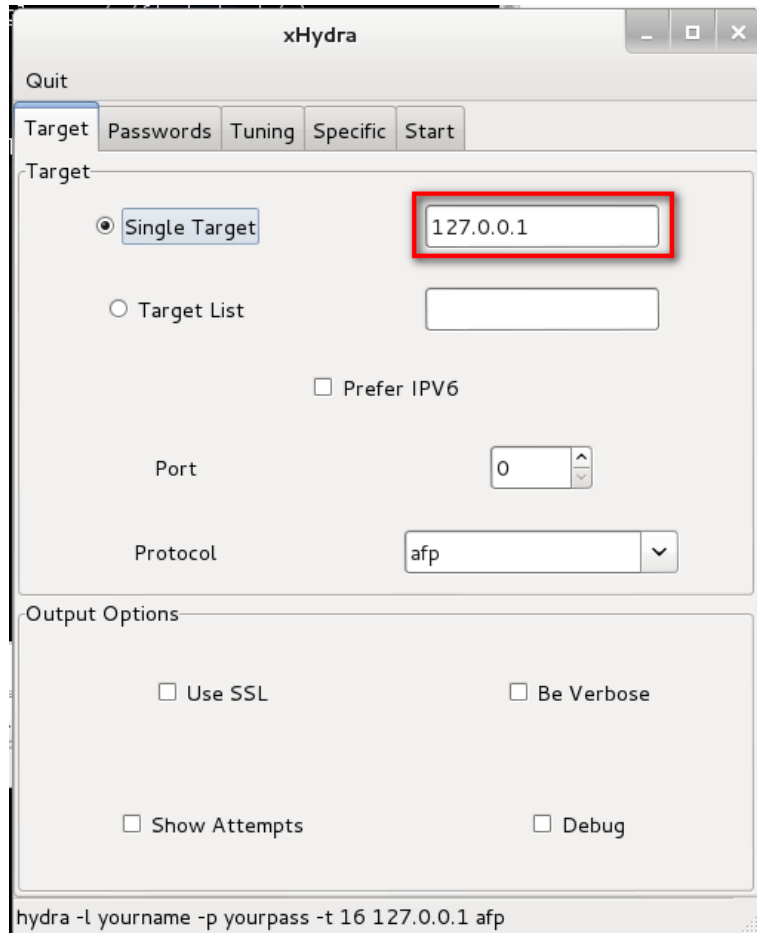
- Online Attack
 - Hydra
- Offline Attack
 - Johnny - GUI for John the Ripper

密碼破解- Hydra

- Hydra 一款密碼破解軟體，它支援許多種通訊協定，並時常更新新的模組。
- Hydra可以在Windows ,OSX, Linux 等環境下執行。



密碼破解- Hydra



The screenshot shows the xHydra application window with the 'Target' tab selected. The 'Single Target' radio button is chosen, and the IP address '127.0.0.1' is entered in the adjacent text field. The 'Port' is set to '0' and the 'Protocol' is set to 'afp'. The 'Output Options' section at the bottom contains several unchecked checkboxes: 'Use SSL', 'Be Verbose', 'Show Attempts', and 'Debug'. The command line at the bottom reads: `hydra -l yourname -p yourpass -t 16 127.0.0.1 afp`.

Quit

Target Passwords Tuning Specific Start

Target

☒ Single Target

☐ Target List

☐ Prefer IPV6

Port

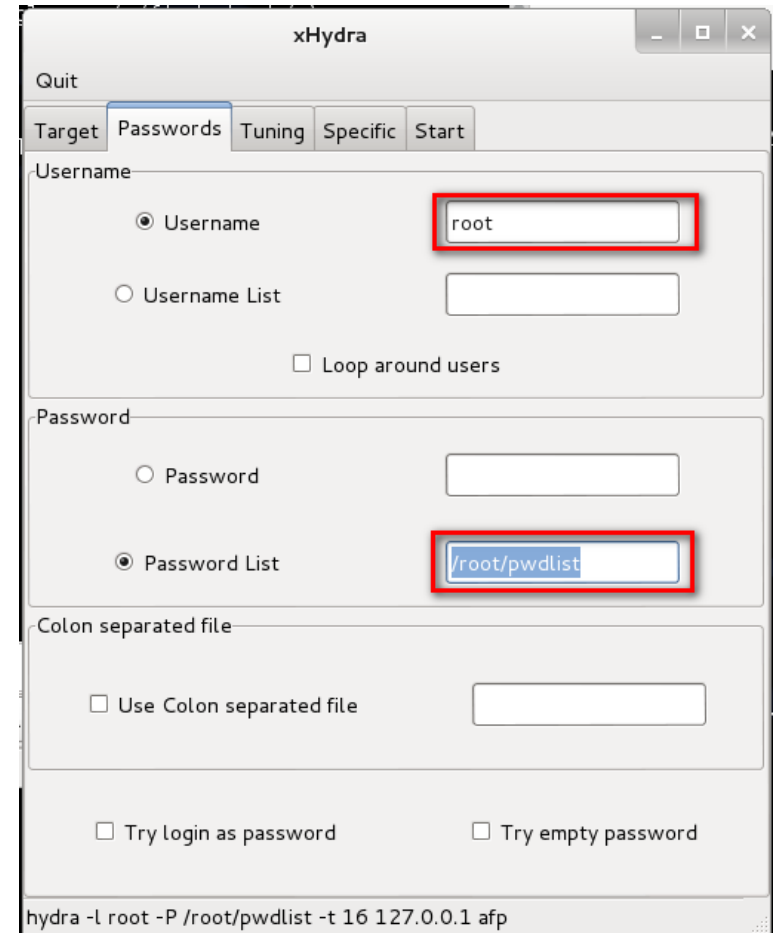
Protocol

Output Options

☐ Use SSL ☐ Be Verbose

☐ Show Attempts ☐ Debug

hydra -l yourname -p yourpass -t 16 127.0.0.1 afp



The screenshot shows the xHydra application window with the 'Passwords' tab selected. Under the 'Username' section, the 'Username' radio button is chosen with 'root' entered in the text field. Under the 'Password' section, the 'Password List' radio button is chosen with '/root/pwdlist' entered in the text field. The 'Colon separated file' section has an unchecked 'Use Colon separated file' checkbox. The bottom section has two unchecked checkboxes: 'Try login as password' and 'Try empty password'. The command line at the bottom reads: `hydra -l root -P /root/pwdlist -t 16 127.0.0.1 afp`.

Quit

Target Passwords Tuning Specific Start

Username

☒ Username

☐ Username List

☐ Loop around users

Password

☐ Password

☒ Password List

Colon separated file

☐ Use Colon separated file

☐ Try login as password ☐ Try empty password

hydra -l root -P /root/pwdlist -t 16 127.0.0.1 afp

我的密碼在哪裡

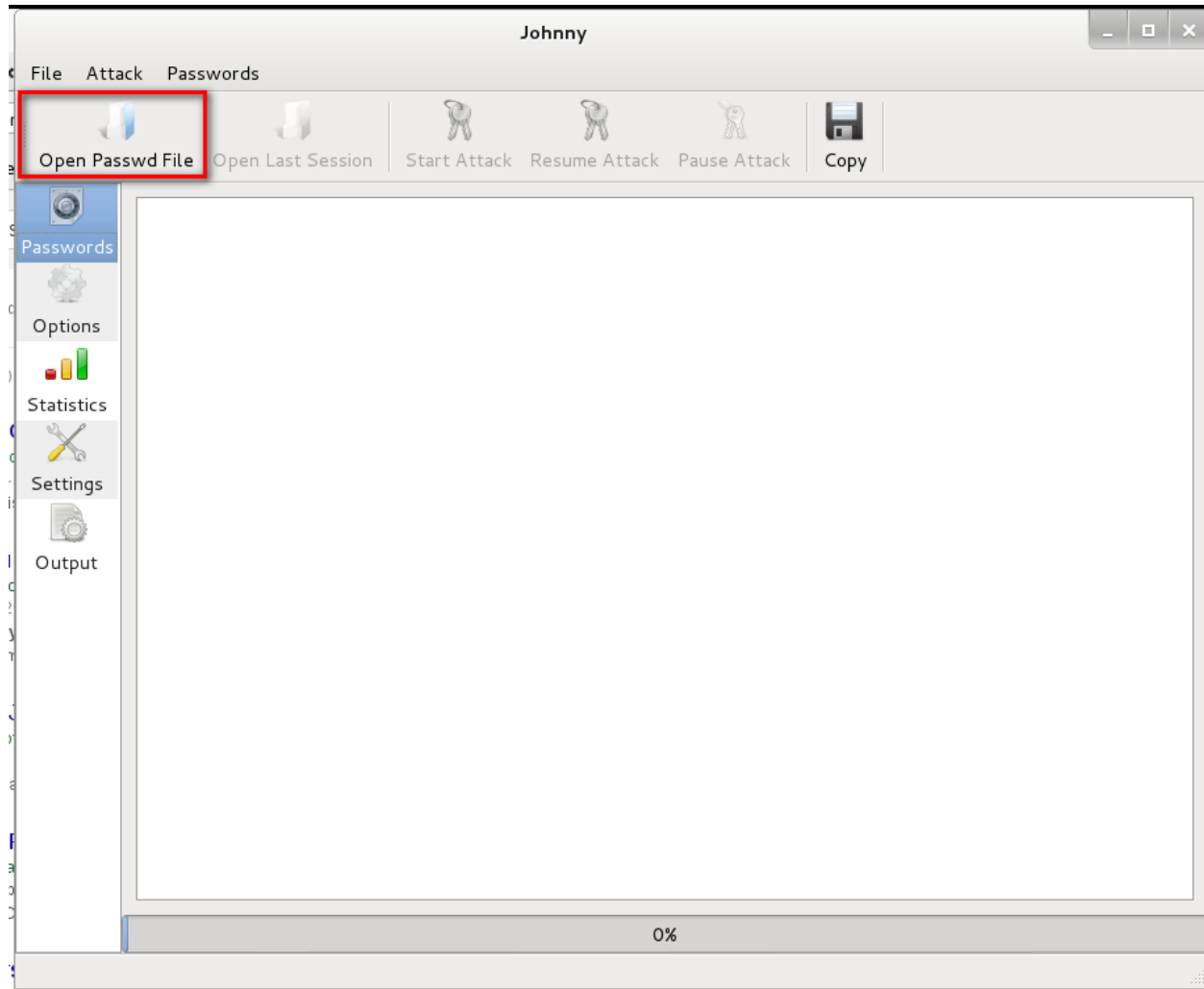
- Windows 密碼檔?
 - C:\winnt\system32\config
- Linux密碼檔?
 - /etc/shadow

密碼破解-John the Ripper

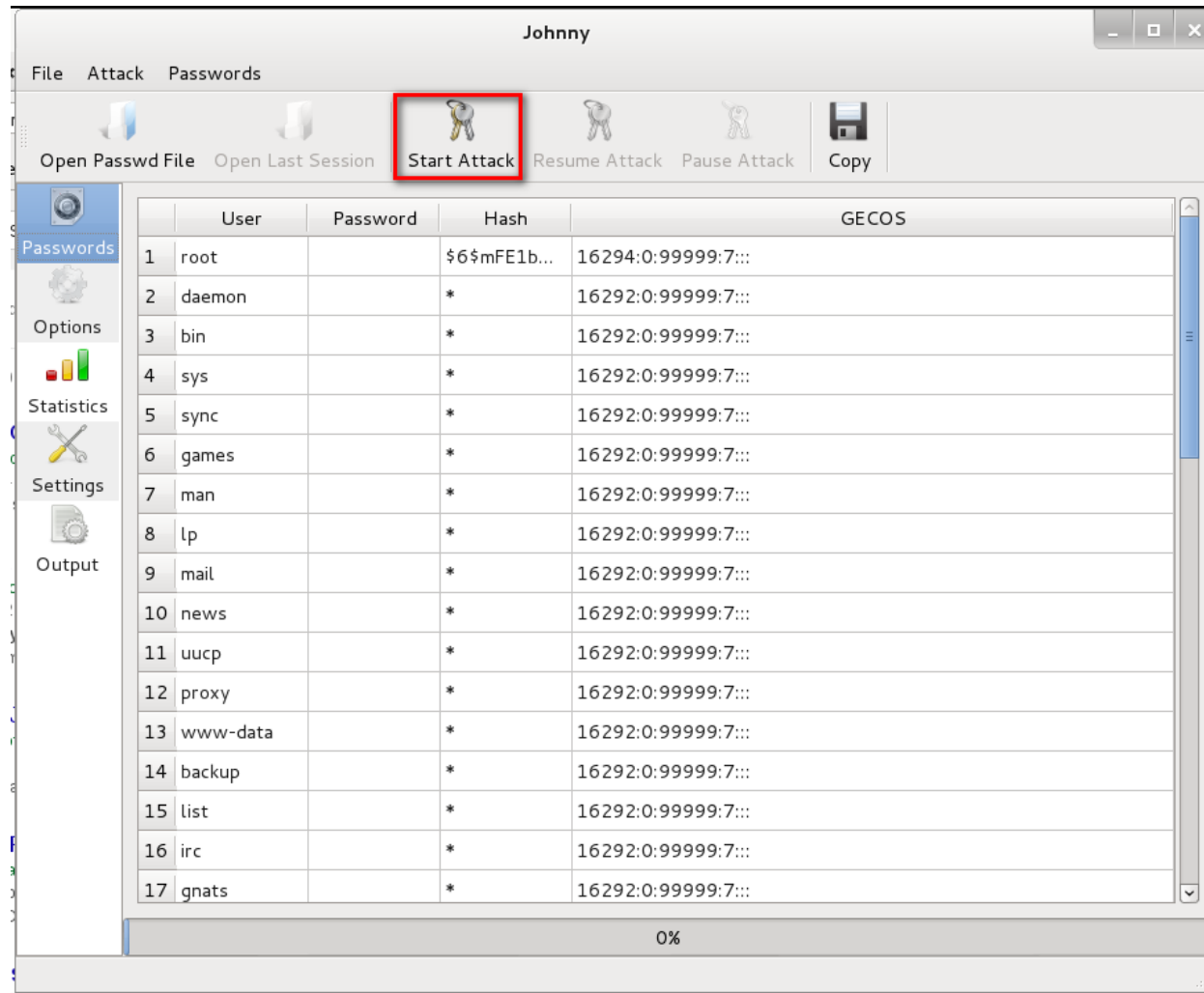
- 一款Open Source的破解密碼軟體，是一個用於在已知密文的情況下嘗試破解出明文的破解密碼軟體，主要支援對DES、MD5 等加密方式的密文進行破解工作。



密碼破解-Johnny



密碼破解-Johnny



密碼破解-Johnny

