網路攻防實務

Agenda

- 資訊安全概論
- 駭客入侵過程簡介
- Ethical Hacking 101

前言

- 隨著網路普及以及數位化資訊社會的到來，資訊科技已經重新定義人類的生活方式以及工作型態。因此，針對自動化運算處理裝置所發展的惡意程式也開始以不同的面貌以及方式開始滲透並影響社會上的每一個個體。

- 網路安全已經成了每一個人都必須要正視的重要議題

聲明

- 以下關於各項弱點原理或攻擊說明僅為教學講解之用，未經其它網站管理人員同意前，嚴禁惡意測試他人網站系統之安全性，否則造成任何法律糾紛皆自行負責。

資訊安全概論

資訊資產的類型

- 資訊資產包含以下範圍：
- 資料(Data)
- 軟體(Software)
- 硬體(Hardware)
- 人員(People)
- 作業流程(Procedure)
- 資訊的類型
- 靜態資訊
- 動態資訊

資訊安全為何？

- 以資源的角度著眼
  - 設備、網路、系統、實體環境、存取控制等
  - 強調在系統架構或平台的安全要求
- 以管理的角度著眼
  - 人員、政策、管理制度等項目
  - 強調在制度面的建立與企業的需求
- 針對資訊的取得進行限制
  - 透過系統資源或是管理制度實現
- 強調縱深防禦
  - 網路架構與防護、系統平台安全、應用軟體安全

資訊安全的基本要素


機密性
Confidentiality
授權
Authorization
可用性
Availability
資安
Information Security
認證
Authentication
完整性
Integrity
不可否認性
No-repudiation

- Confidentiality
  - a set of rules or a promise that limits access or places restrictions on certain types of information
- Integrity
  - maintaining and assuring the accuracy and consistency of data over its entire life-cycle
- Availability
  - the information or service must be available when it is needed.

- No-repudiation
  - one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction
- Authentication
  - the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity
- Authorization
  - the function of specifying access rights to resources related to information security and computer security

資訊安全的威脅

- 環境的威脅:(15%~17%)
  - 火災(10%~12%)
  - 水災(5%~7%)
- 意外性災害如地震(比例低，但發生會釀成巨禍)
- 利用建築物等外在保護或備份

- 人的威脅:(83%~85%)
  - 內部人員(70%~85%)
    - 人為疏忽及犯錯(50%~60%)
    - 不誠實的員工(10%)
    - 心懷怨恨的員工(10%)
  - 外部人員(3%~5%)
    - 網路駭客、電腦病毒、被竊聽等等
- 利用資訊安全技術保護

資訊安全十大領域

- Access Control 存取控制
  - 存取控制之定義與觀念
  - 系統與資料之存取控制
  - 入侵偵測及防禦系統
  - 確保存取控制之施行
  - 身份識別與認證

資訊安全十大領域

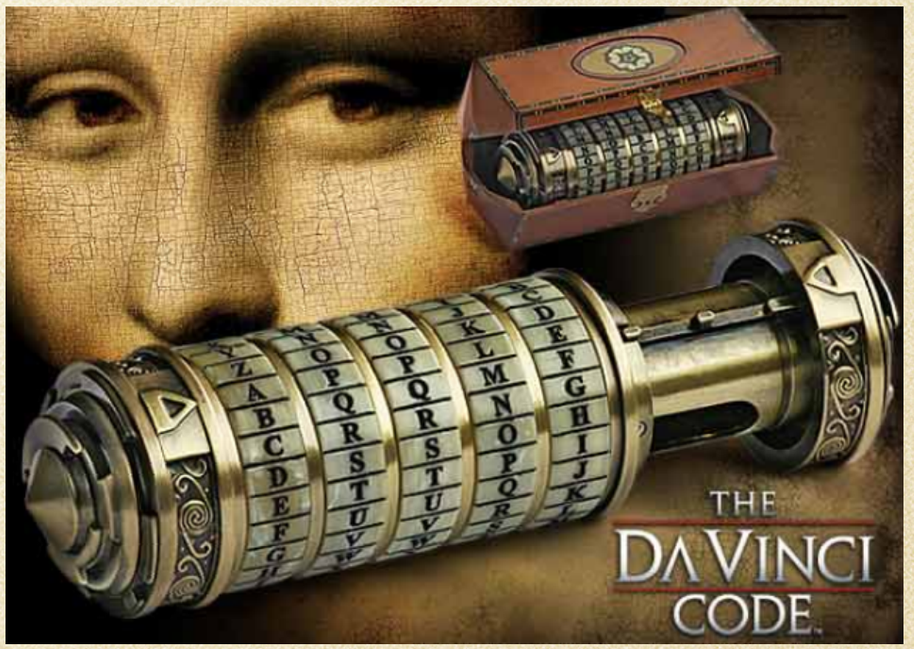
- Application Security 應用程式安全
  - 惡意程式與威脅
  - 軟體防護措施
  - 資料庫安全性
  - SQL Injection
  - 網站系統安全性

資訊安全十大領域

- Business Continuity and Disaster Recovery Planning 業務持續性與災害復原
  - 瞭解持續營運計畫建立之過程
  - 整合持續營運計畫至企業組織
  - 定義持續營運計畫之執行過程

資訊安全十大領域

- Cryptography 密碼學
  - 密碼學觀念之建立
  - 密碼演算法之運作與應用
  - 訊息完整性檢查與數位簽章
  - 數位憑證
  - 破密分析
  - Rainbow Table



資料來源：The Davinci Code

資訊安全十大領域

- Information Security and Risk Management 資訊安全與風險管理
  - 資訊安全之需求與原則
  - 資訊安全政策、程序、標準與基準
  - 組織中人員的角色與責任
  - 風險管理
  - 道德規範

資訊安全十大領域

- Law, Regulations, Compliance, and Investigations 法律、規章、遵循性與調查
  - 國際間之法律系統
  - IT相關之法令與規章
  - 安全事件回應
  - 犯罪調查

資訊安全十大領域

- Operations Security 操作安全
  - 資訊系統之防護與管理
  - 系統異動管理
  - 特權個體之控管

資訊安全十大領域

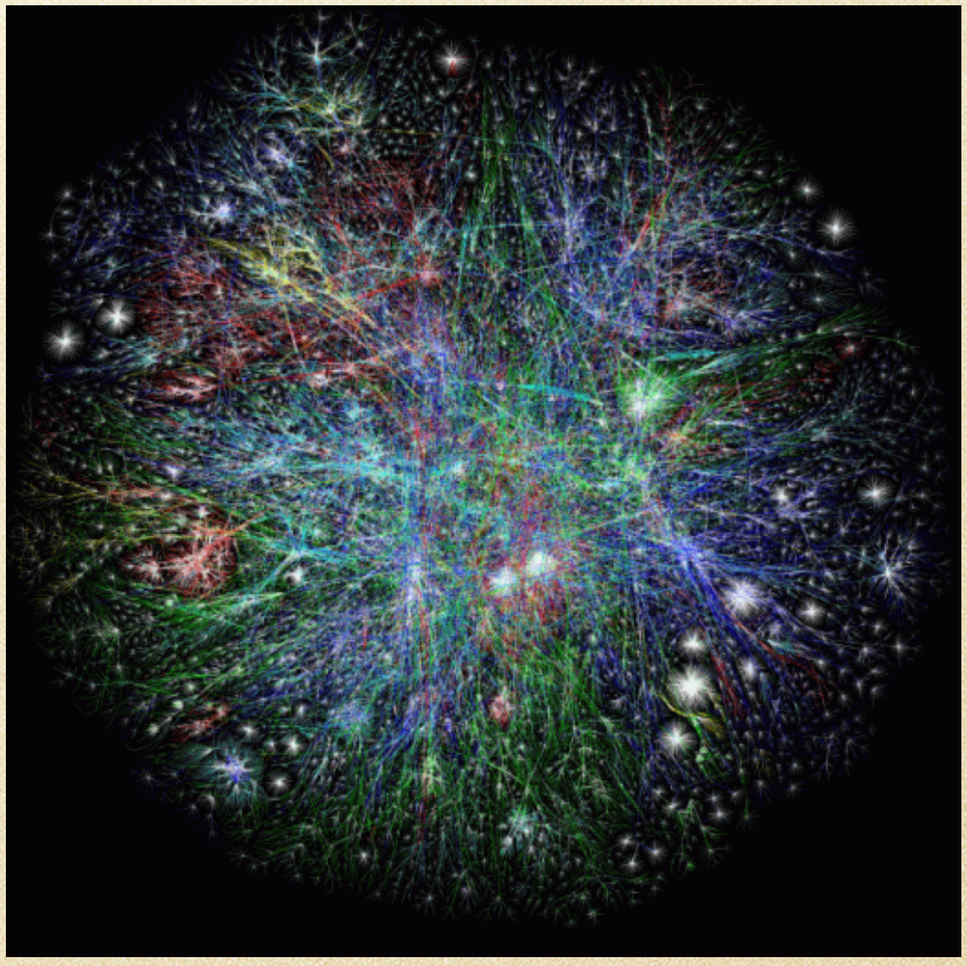
- Physical (Environmental) Security 實體(環境)安全
  - 縱深防禦
  - 實體安全控制措施
  - 公共設施之安全問題

資訊安全十大領域

- Security Architecture and Design 安全架構與設計
  - 企業資訊安全架構
  - 系統安全架構
  - 受信任運算基礎
  - 安全模型

資訊安全十大領域

- Telecommunications and Network Security 通訊與網路安全
  - 通訊協定之安全性
  - 區域網路之安全性
  - 廣域網路之安全性
  - 無線網路之安全性
  - VoIP之安全性
  - 網路服務之安全性



資訊安全十大領域

- 惡意程式大量出現，自動化攻擊模式影響範圍廣
- 須同時兼顧系統、網路、應用程式與架構上的安全設計
- 從事件調查看資安問題
- 新型態的攻擊層出不窮
- 傳統安全防禦機制失靈
- 複雜且難以管理的安全政策
- 身份認證機制
- 無線通訊的安全問題

What’s Ethical Hacker

https://github.com/daryllxd/lifelong-learning/blob/master/how-to-become-a-hacker.md

資安網址好站分享

- THE Hack News
  - https://thehackernews.com
- Zero-day.HITCON
  - https://zeroday.hitcon.org
- FREEBUF
  - http://www.freebuf.com
- Exploit Database
  - https://www.exploit-db.com

如何學習與瞭解

- 國際組織
  - The Honeynet Project、Cloud Security Alliance、FIRST、Shadowserver Foundation…
- 國際會議
  - The Honeynet Project Annual Workshop、Cloud Security Alliance Congress、RSA、Blackhat、DEFCon、AVAR
- 國內社群
  - RAT、SHIELD
- 參加國內會議
  - HITCON、資安研討會
- 主辦國內會議
  - HoneyCon、CSA Taiwan、IRCON

駭客手法入侵過程簡介

電影中你發現了什麼


Data Breach
Cyber Attack
Protection
System Safety Compromised

如何進行

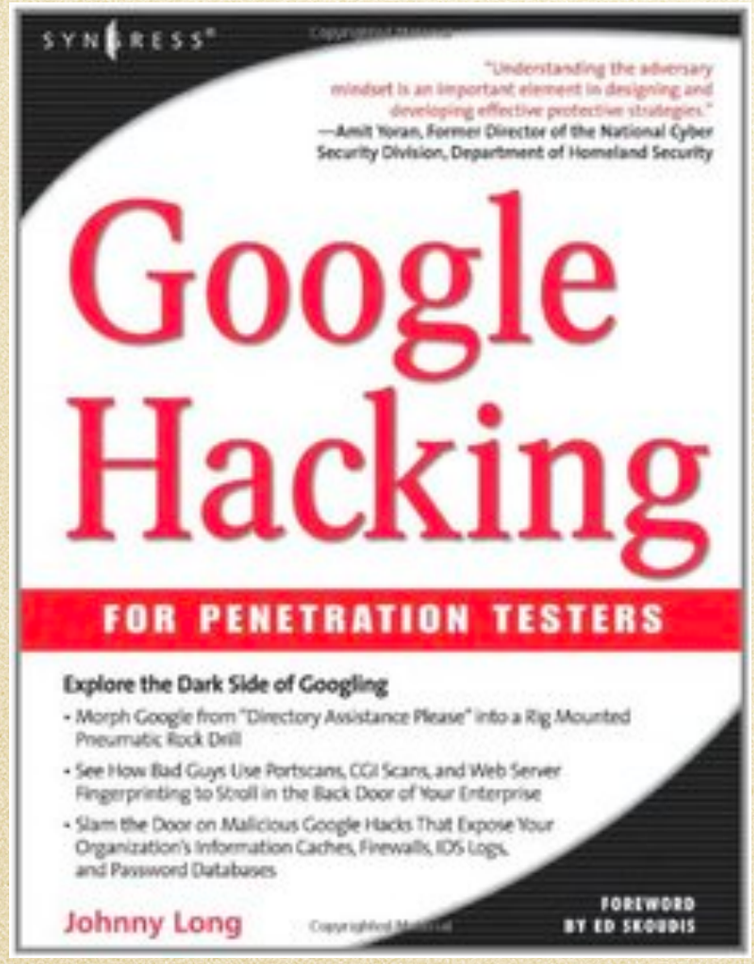
他們如何研究目標呢？

如何進行探測？

所謂的老方法是什麼呢？

如果是你，你會怎麼攻擊呢?

Google Hacking



交通與聯絡資訊 - 國網中心

https://www.nchc.org.tw/posts/AGW1mlivFC/交通與聯絡資訊

intitle

inurl

site

intext

尋找特定檔案類型：filetype

上班時間：週一至週五09:00~17:00

財團法人國家實驗研究院

國家高速網路與計算中心

National Center for High-performance Computing

0800-351-510

傅真：

886-3-57

設施服務 技術研發 中心 關於我們

組織架構

主任室

大事記要

交通與聯絡資訊

人才招募

專利與技術轉移

參觀服務

場地租借

教育訓練

相關連結

台中分部

地址：

40763 台
號

電話：

886-4-2462-0202、886-4-2465-0818

傳真：

886-4-2462-7373

台中分部

台南分部

Exploits Database by Offensive

https://www.exploit-db.com

EXPLOIT DATABASE

Verified | Has App

Filters | Reset All

Show 15

Search:

Date	D	A	V	Title	Type	Platform	Author
2018-11-27	⬇		✓	Netgear Devices - Unauthenticated Remote Command Execution (Metasploit)	Remote	Hardware	Metasploit
2018-11-26	⬇		✓	Xorg X11 Server - SUID privilege escalation (Metasploit)	Local	Multiple	Metasploit
2018-11-26	⬇	📦	✗	Arm Whois 3.11 - Buffer Overflow (ASLR)	Local	Windows_x86	zephyr
2018-11-26	⬇	📦	✗	ELBA5 5.8.0 - Remote Code Execution	Remote	Windows	Florian Bogner
2018-11-26	⬇		✗	Zyxel VMG1312-B10D 5.13AAXA.8 - Directory Traversal	WebApps	Hardware	numan türle
2018-11-26	⬇	📦	✗	No-Cms 1.0 - 'order_by' SQL Injection	WebApps	PHP	Loading Kura Kura
2018-11-26	⬇		✗	Ticketly 1.0 - 'kind_id' SQL Injection	WebApps	PHP	Javier Olmedo
2018-11-26	⬇		✗	MariaDB Client 10.1.26 - Denial of Service (PoC)	DoS	Linux	strider
2018-11-26	⬇	📦	✗	WordPress Plugins Easy Testimonials 3.2 - Cross-Site Scripting	WebApps	PHP	En_dust
2018-11-26	⬇		✗	Ricoh myPrint 2.9.2.4 - Hard-Coded Credentials	WebApps	Hardware	Hodorsec
2018-11-21	⬇	📦	✗	WebOfisi E-Ticaret V4 - 'urun' SQL Injection	WebApps	PHP	AkkuS
2018-11-21	⬇		✗	WordPress CherryFramework Themes 3.1.4 - Backup File Download	WebApps	PHP	b1p0l4r

https://www.exploit-db.com

Google Hacking Database

https://www.exploit-db.com/google-hacking-database

EXPLOIT DATABASE

Google Hacking Database

Filters | Reset All

Show 15

Quick Search

Date Added	Dork	Category	Author
2018-11-28	"inurl:"Umbraco/#/login" site:*edu"	Pages Containing Login Portals	CrimsonTorso
2018-11-28	"site:ghostbin.com " / " "	Files Containing Juicy Info	CrimsonTorso
2018-11-28	"site:hastebin.com " / " "	Files Containing Juicy Info	CrimsonTorso
2018-11-27	intitle:'index of' "error_log"	Sensitive Directories	Brain Reflow
2018-11-27	intitle:'index of' "access_log"	Sensitive Directories	Brain Reflow
2018-11-27	inurl:/certsrv/certrqus.asp	Various Online Devices	Mattias Borg
2018-11-27	inurl:/config/authentication_page.htm	Pages Containing Login Portals	ManhNho
2018-11-27	intext:"Type in Username and Password, then click Ok" intitle:"log in"	Pages Containing Login Portals	ManhNho
2018-11-27	intitle:"index of /" intext:/backup	Sensitive Directories	Mattias Borg
2018-11-21	"syd_apply.cfm"	Error Messages	CrimsonTorso
2018-11-20	inurl:/wp-content/uploads/wp-backup-plus/	Sensitive Directories	PUNIT DARJI
2018-11-16	intitle:"index of /" authorized_keys	Sensitive Directories	nuria_pp
2018-11-15	index of kcfinder/	Sensitive Directories	ManhNho

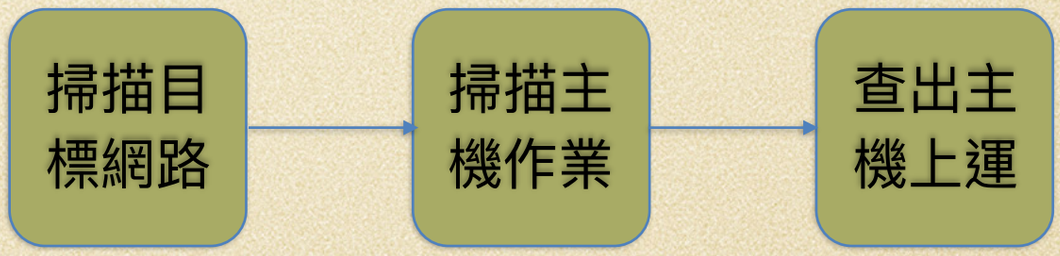
GHDB,https://www.exploit-db.com/google-hacking-database

Ethical Hacking 101

網路端口掃描

- 什麼是掃描？
  - 掃描為駭客入侵的第二大步驟
  - 掃描有助於了解全盤網路架構及服務資訊

- 網路掃描可以找到哪些資訊呢？
  - IP address
  - 作業系統
  - 系統架構
  - 線上運行的服務
  - ….



網路端口掃描

- 掃描分為幾大類
  - Port Scanning (通訊埠端口掃描)
  - Network Scanning (網路架構掃描)
  - Vulnerability Scanning （弱點掃描）

網路端口掃描

- Port Scanning
  - 端口掃描有助了解電腦運行了哪些服務 ，如檔案伺服器（Port21）、網頁伺服器（Port 80）
- Network Scanning
  - 網路掃描為識別網路上活動主機的程序，並有助於網路安全評估
- Vulnerability Scanning
  - 弱點掃描可以了解目前網路環境及運行主機上存在哪些系統及應用程式相關漏洞

常見的通訊協定

- 什麼是埠口（Port)?
  - port 就是一個服務的端口,就如同郵局或銀行一樣,每個服務櫃檯都有相對應提供的服務,例如： 1號窗口提供存款及提款的服務 、2號窗口提供領取中獎發票獎金的服務等等.
- 那有多少的Port 呢？
  - 0~65535
- Well-Known Ports
  - 0~1023
- Dynamic Ports
  - 1024~65535

常見的通訊協定

PortNumber	名稱	說明
20	ftp-data	ftp資料連接埠
21	ftp	檔案傳輸協定（ftp)連接埠
22	ssh	Secure Shell
23	telnet	Telnet
25	smtp	Simple Mail Transfer Protocol
53	domain	網域名稱服務
69	tftp	TFTP
80	http	www 服務
110	pop3	mail 通訊協定

常見的通訊協定

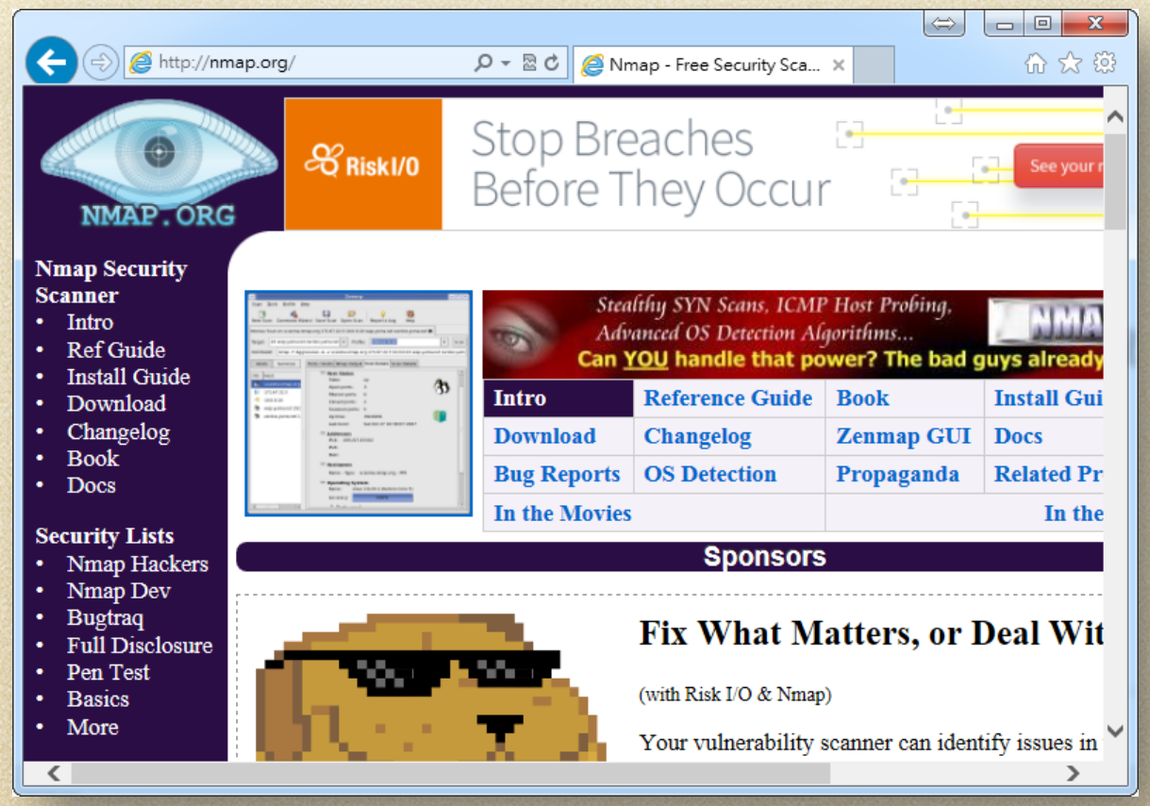
PortNumber	名稱	說明
115	sftp	安全的檔案傳輸協定
123	ntp	網路時間協定
137	netbios-ns	netbios 名稱服務
138	netbios-dgm	netbios資料包服務
139	netbios-dgm	netbios工作階段服務
143	imap	網際網路訊息存取協定
443	https	https
445	microsoft-ds	透過tcp/ip的smb
1433	ms-sql-s	ms sql server

常見的通訊協定

PortNumber	名稱	說明
3306	*mysql*	*mysql server*
3389	*rdp*	*windows 遠端桌面*
8080	*http*	*www 服務*
8443	*https*	*https*

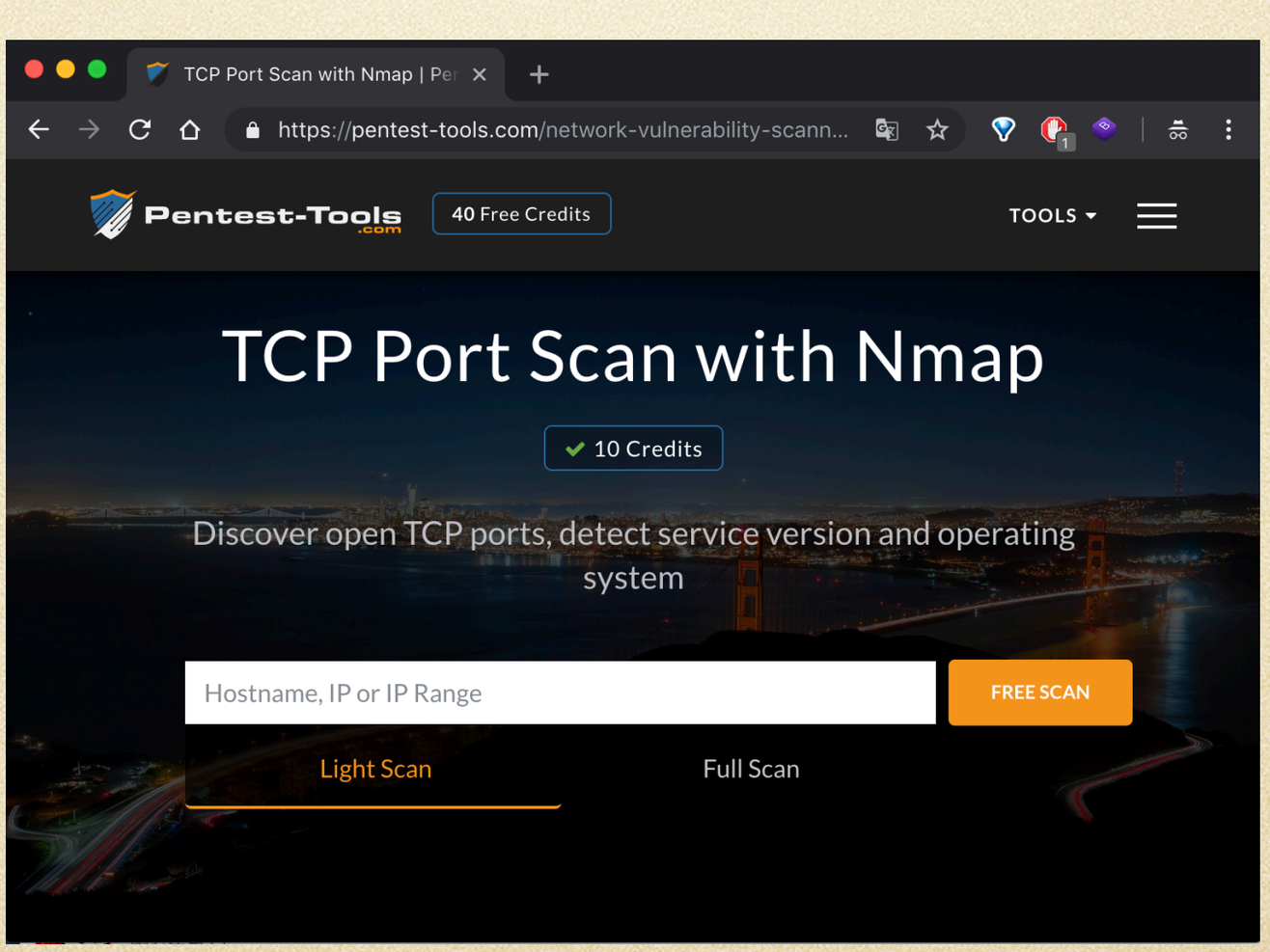
網路與主機掃瞄-Nmap

- 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



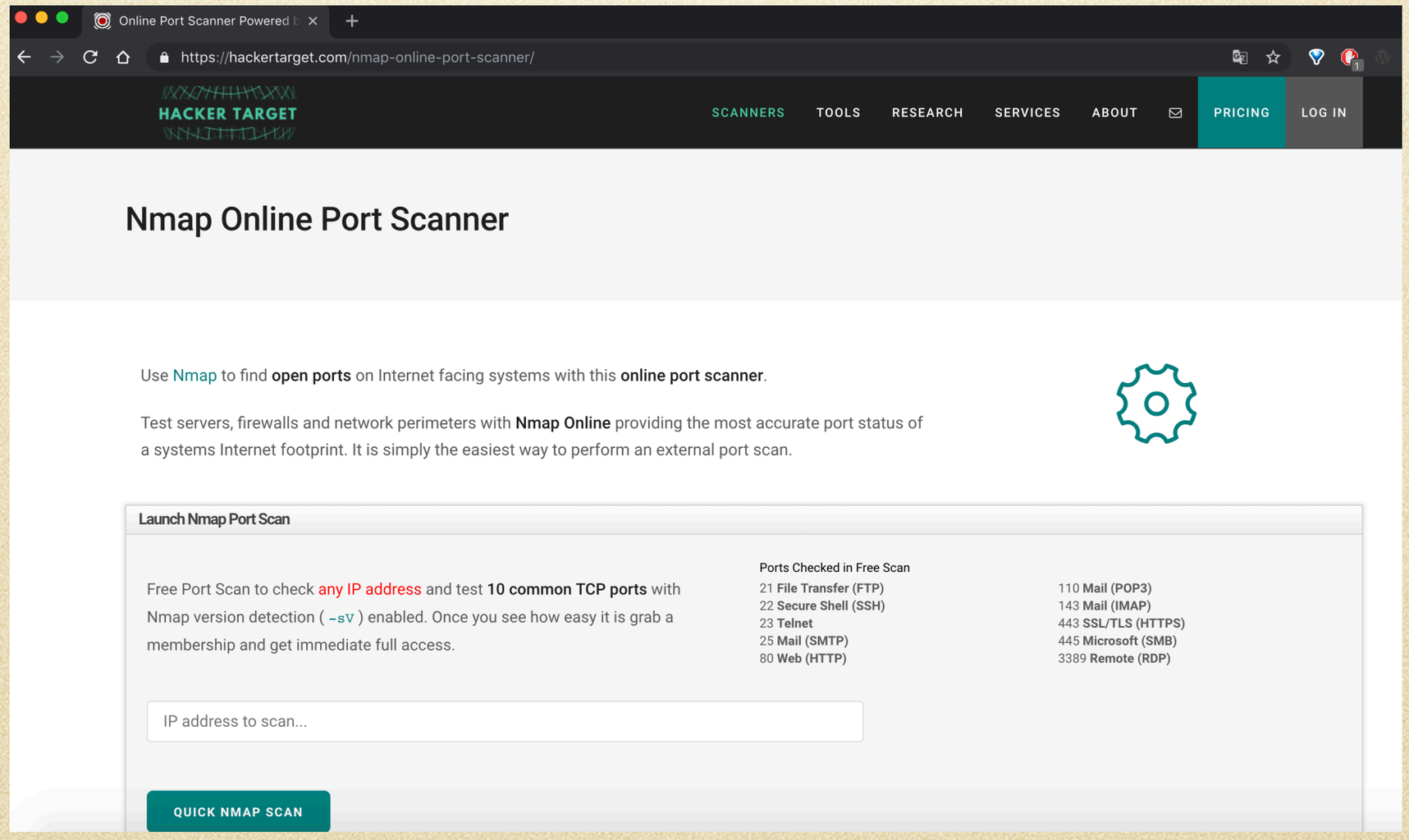
Online tools (1/2)

- https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap

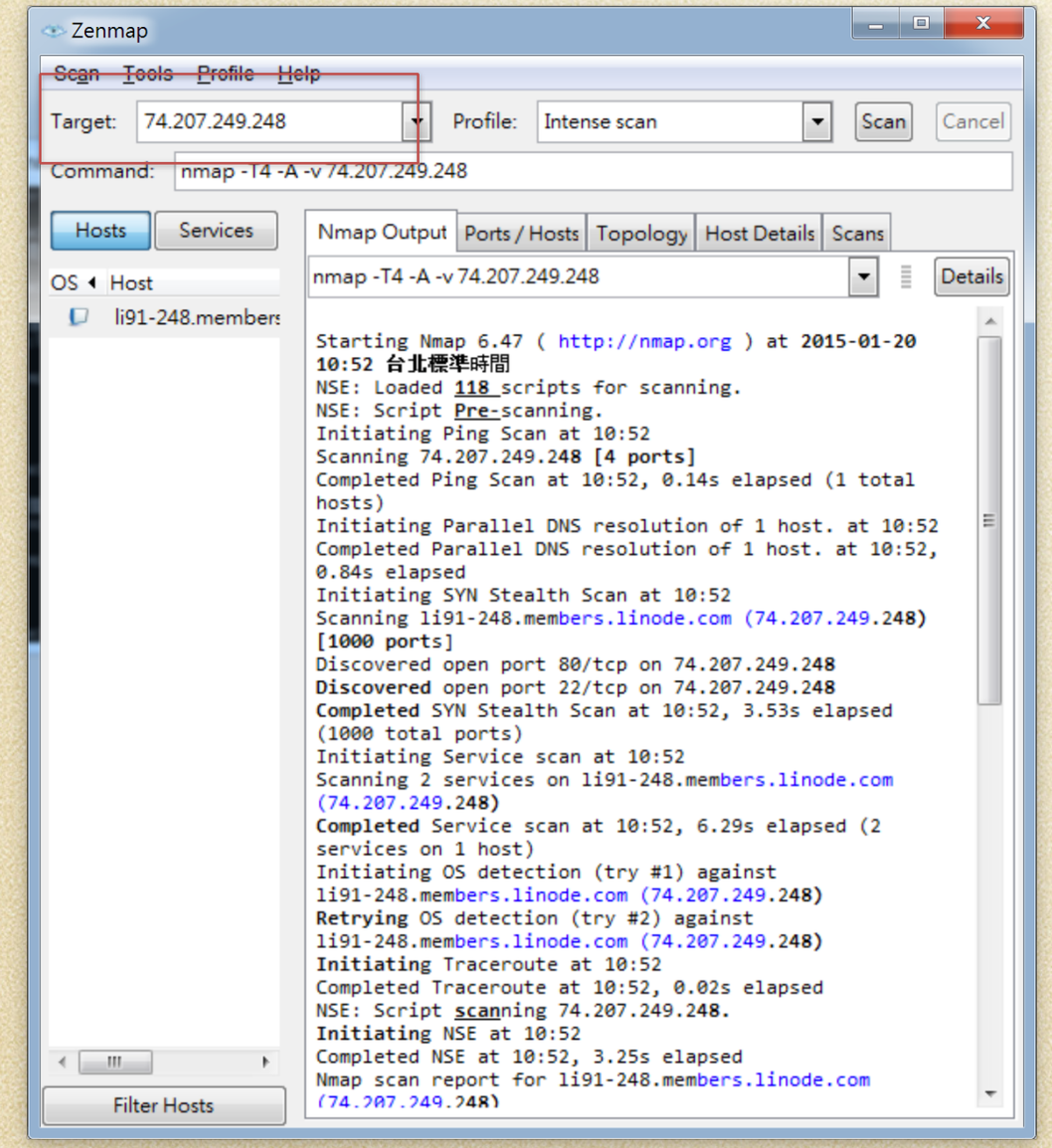


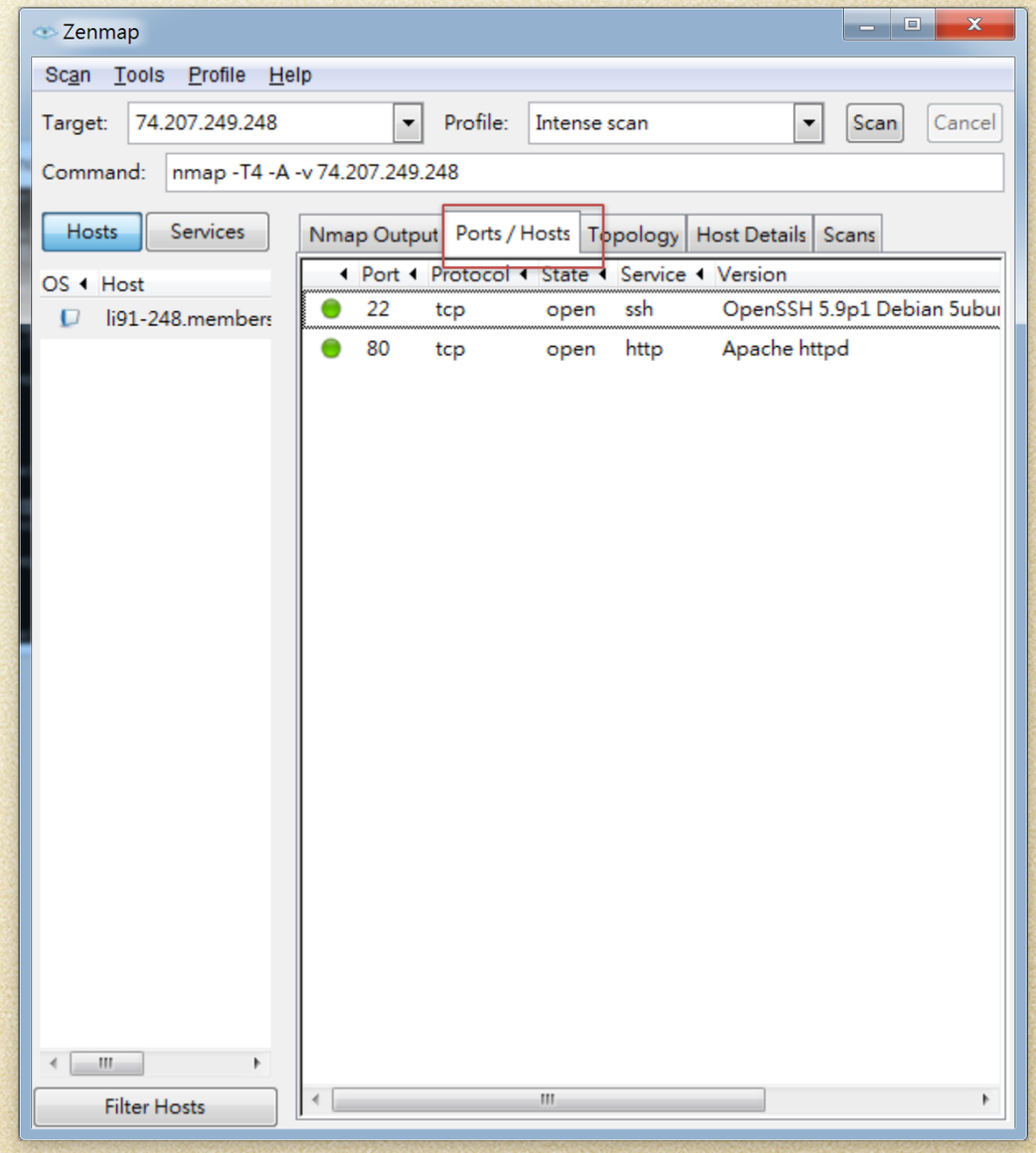
Online tools (2/2)

- https://hackertarget.com/nmap-online-port-scanner/

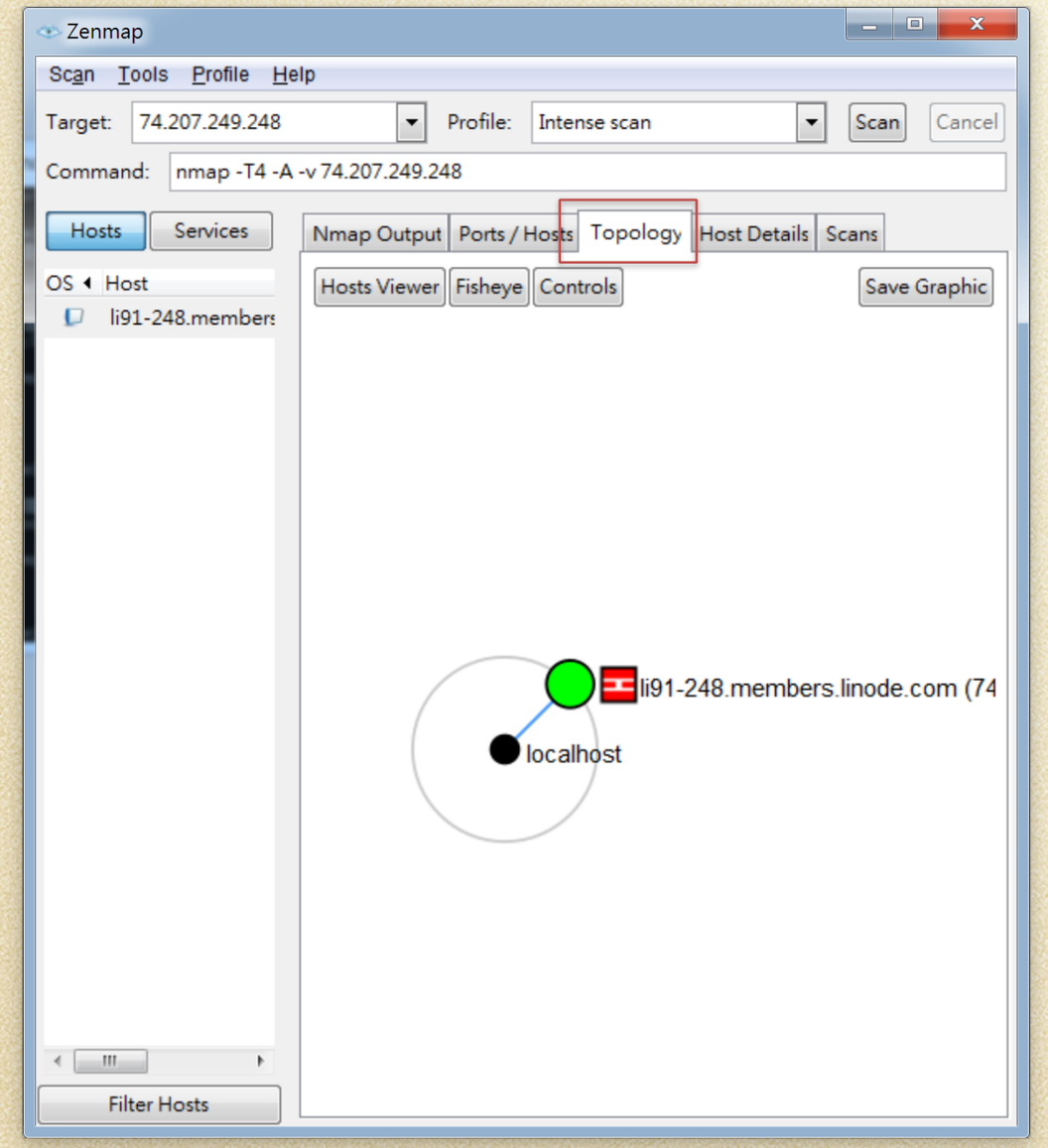


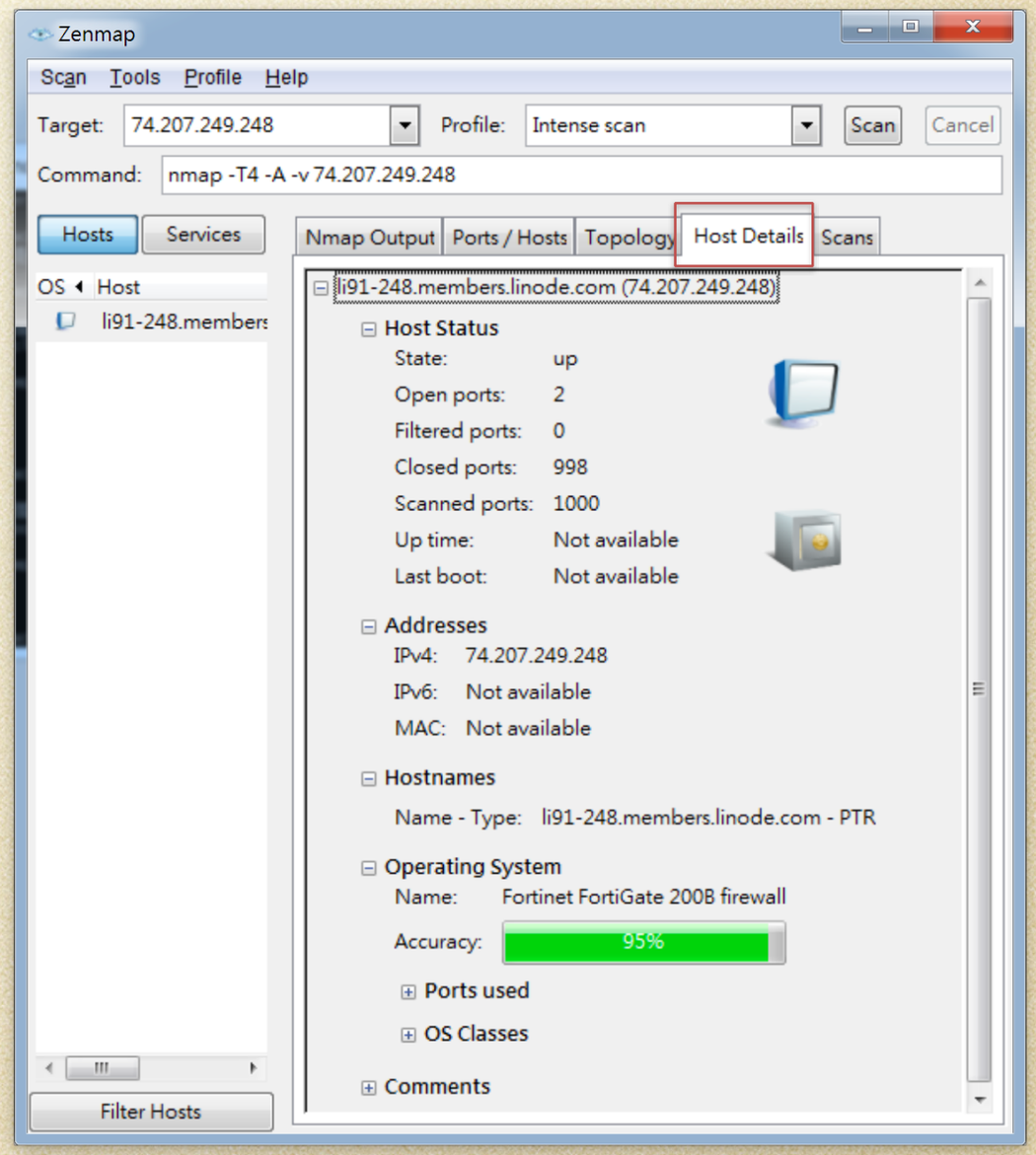
網路與主機掃瞄-Nmap



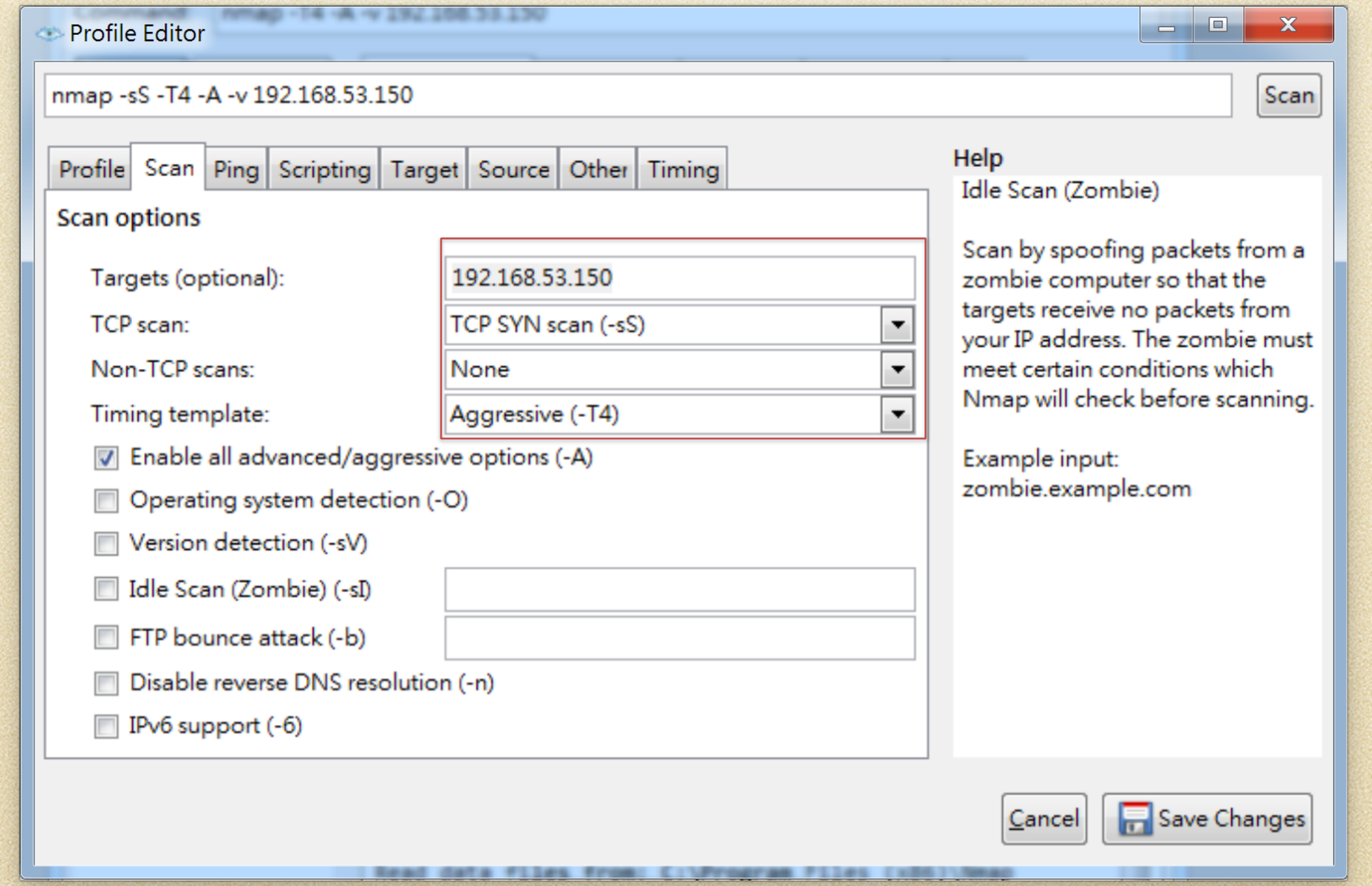


網路與主機掃瞄-Nmap

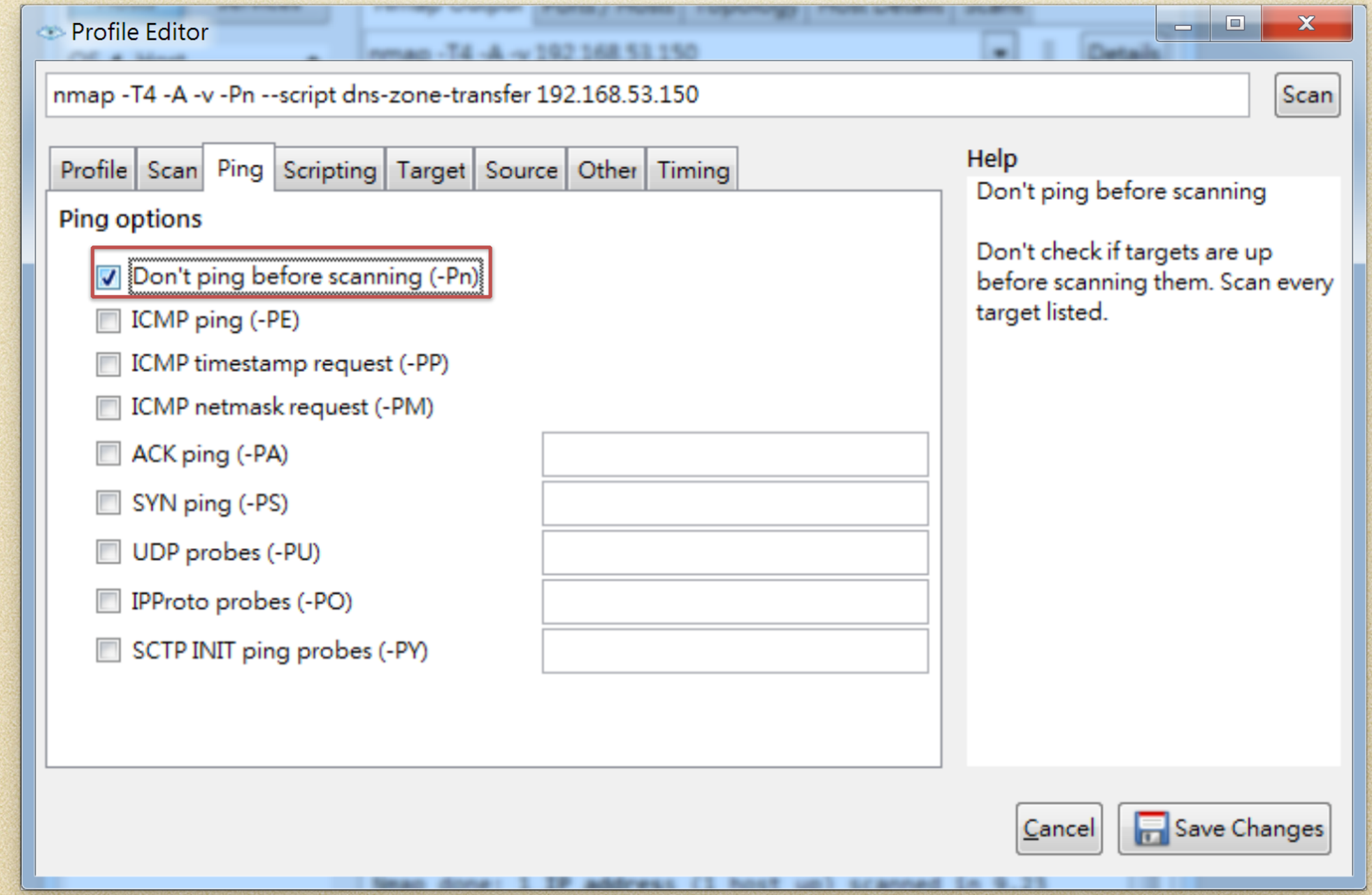




網路與主機掃瞄-Nmap

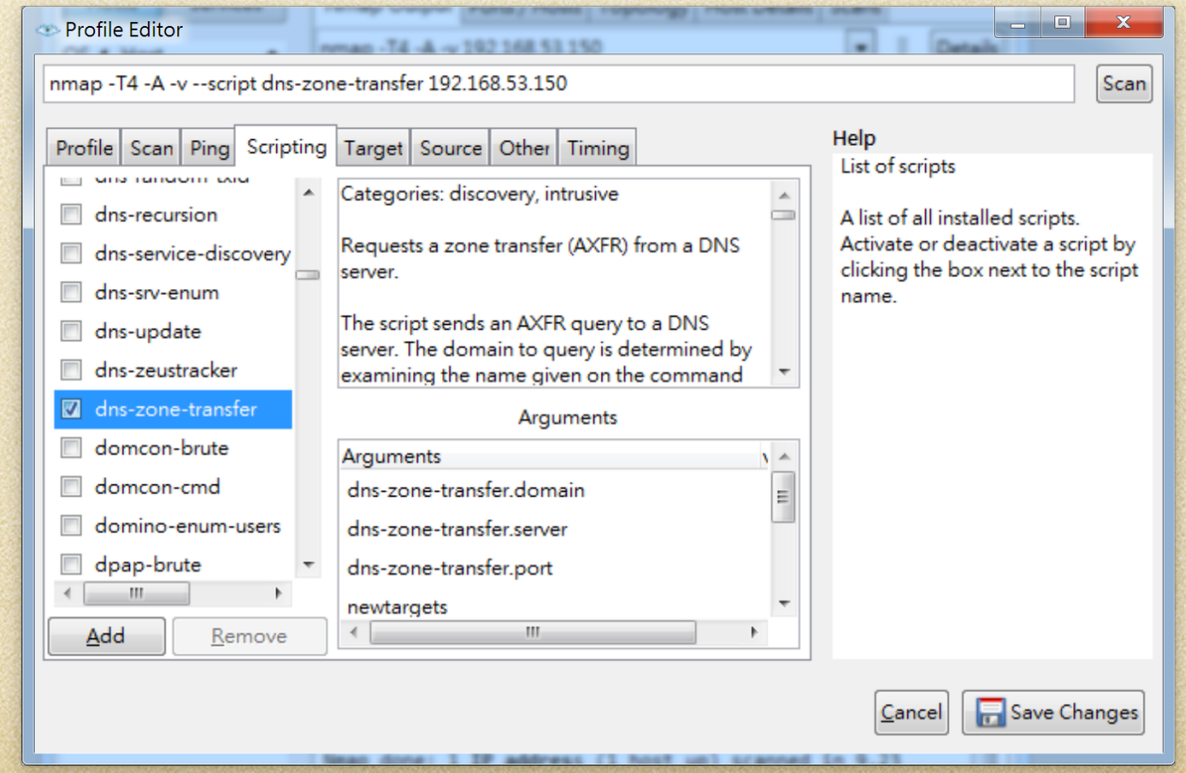


網路與主機掃瞄-Nmap



NSE Scripts

- 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。



Fing

fing

Fingbox Partner Support Blog BUY NOW Web App

Troubleshoot and secure your home network with the Fing app and Fingbox sensor.

Download the free app today.

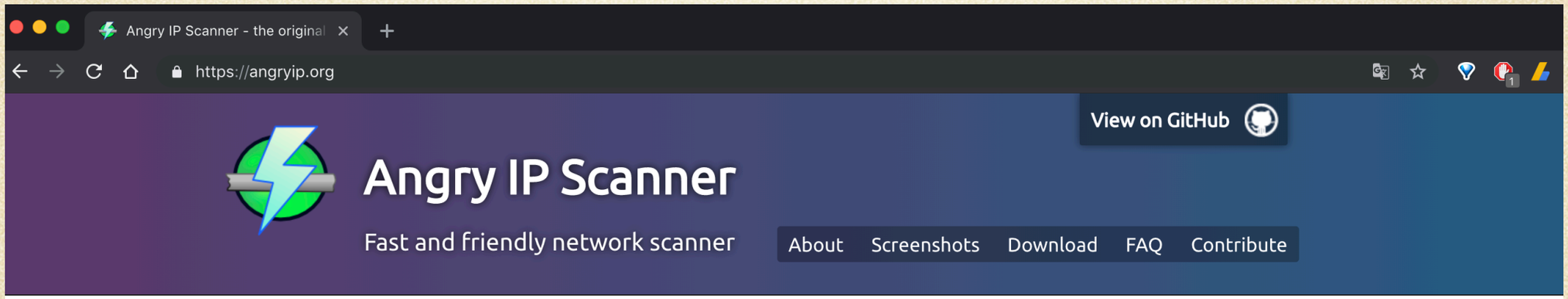
GET IT ON Google Play

Download on the App Store

Buy Fingbox

Learn More

Angry IP

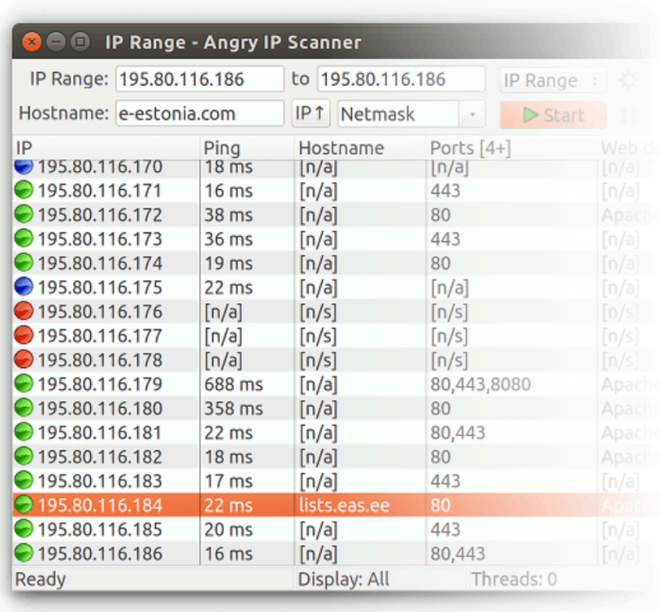


Features

- Scans local networks as well as Internet
- IP Range, Random or file in any format
- Exports results into many formats
- Extensible with many data fetchers
- Provides command-line interface

- Over 23 million downloads
- Free and open-source
- Works on Windows, Mac and Linux
- Installation not required

Free Download



Description

Angry IP Scanner (or simply ipscan) is an open-source and cross-platform network scanner designed to

弱點分析

- 用來檢查網路或作業系統的安全性
- 模擬攻擊者所發出的攻擊動作
- 可提供網路管理人員做為弱點修補之依據，以提昇安全性
- 與防毒軟體的做法相似，依據所謂的「弱點特徵資料庫」來測試是否存在已知的漏洞

弱點分析

- 弱點掃描器透過預先載入的系統漏洞資訊對目標資訊設備進行模擬攻擊。
- 弱點掃描的4個階段：
  - 主機探索
  - 連接埠掃描
  - 系統服務確認
  - 漏洞探測
  - 安全評估結果產出

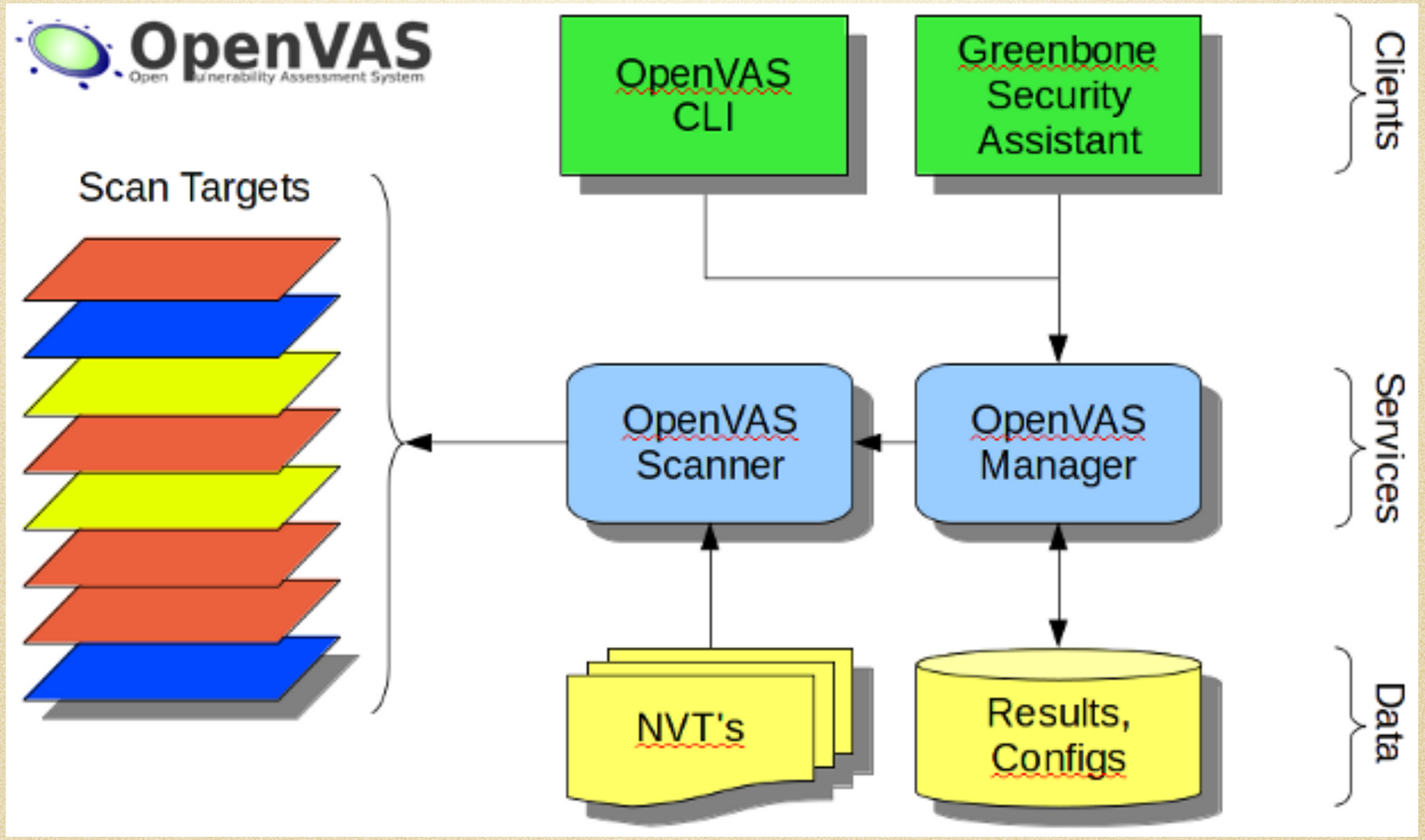
常見的弱點評估軟體

- 針對系統服務的弱點評估
  - Nessus(http://www.tenable.com/products/nessus)
  - Openvas (http://www.openvas.org/)
- 針對Web 應用程式的弱點評估
  - O-scan (http://www.wesoft.info/download.php)
  - Vega (https://subgraph.com/vega/)
  - W3af(http://w3af.org/)

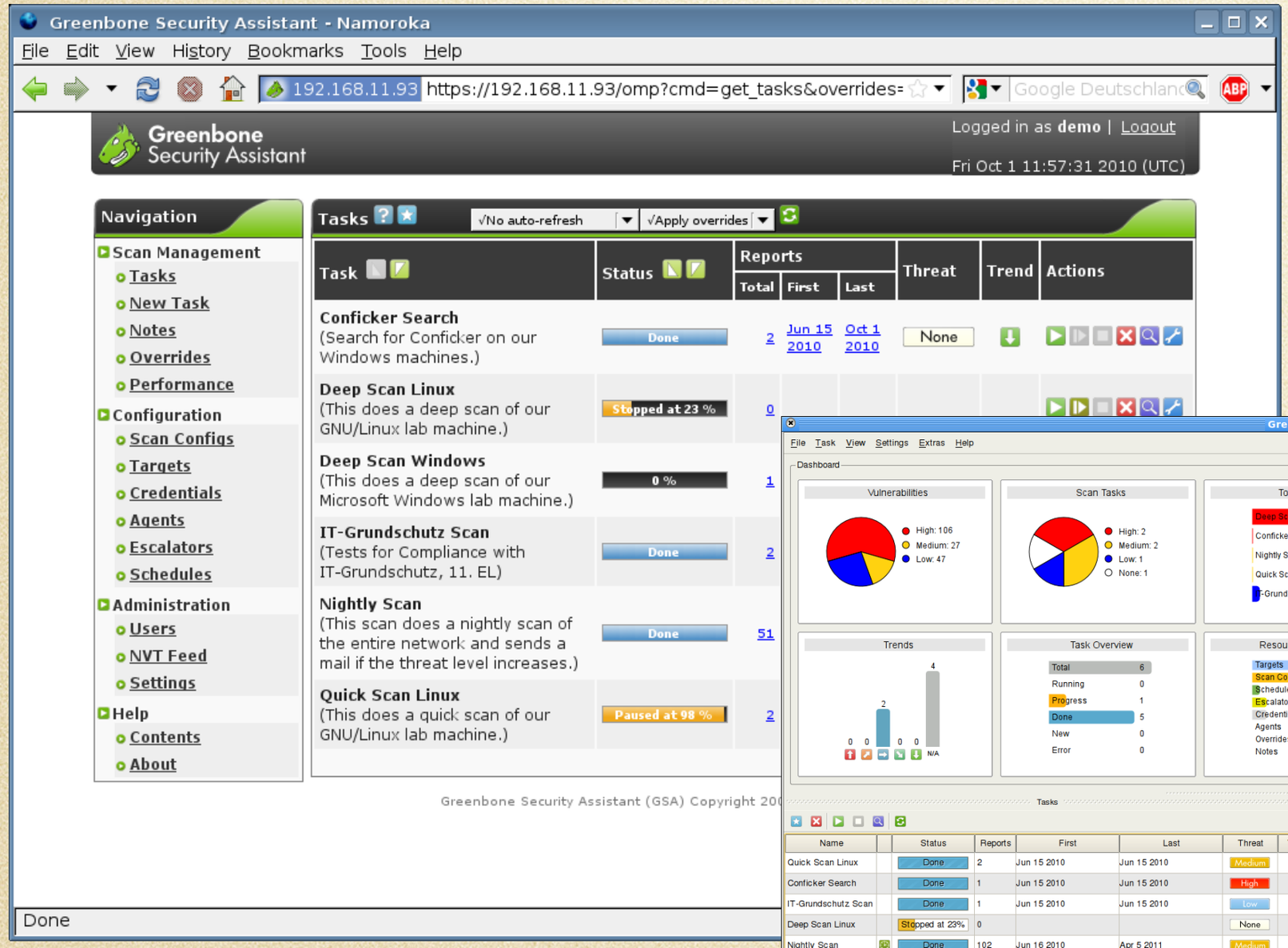
OpenVAS 介紹

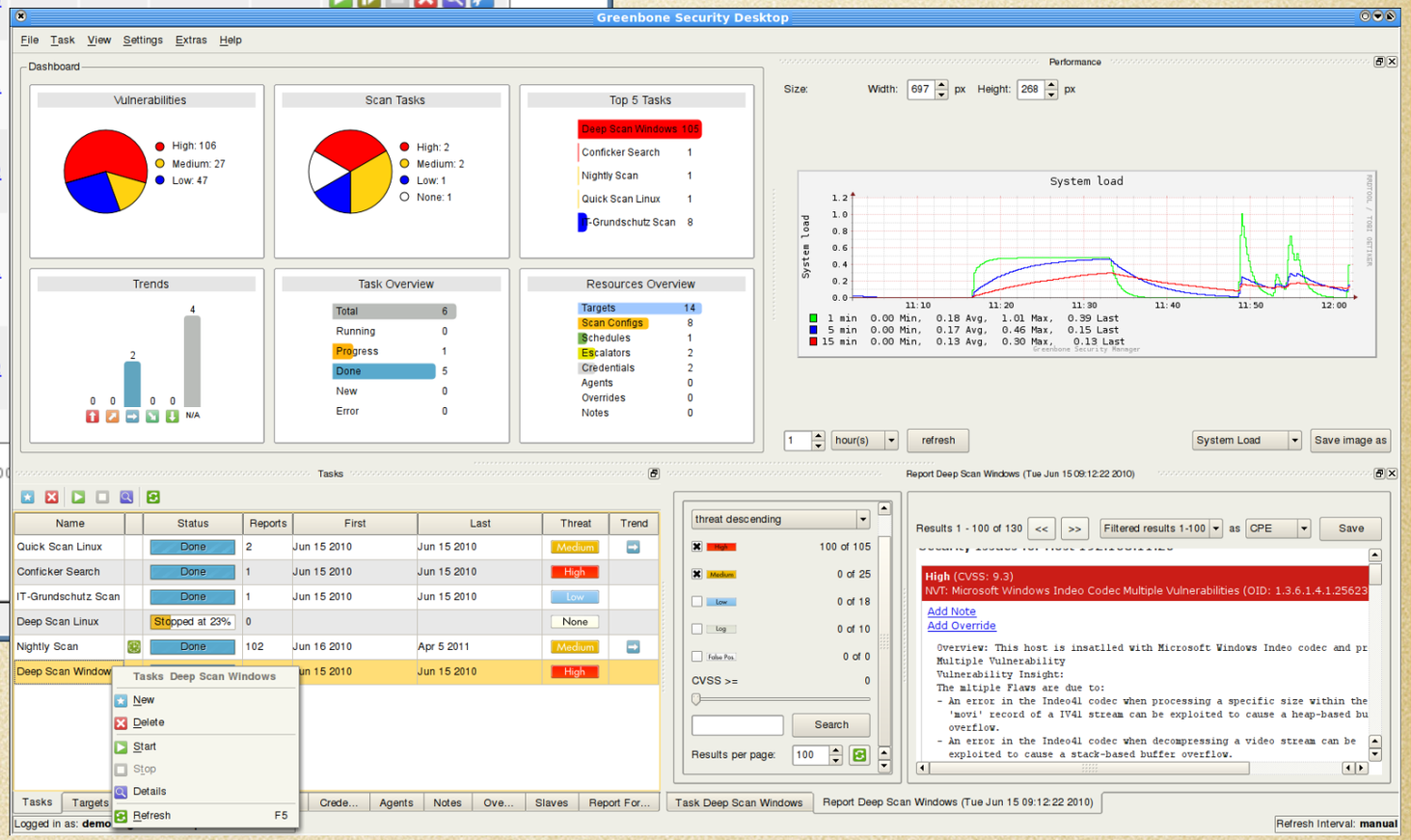
- OpenVAS 為一套全面且強大的漏洞掃描及管理解決方案的一個框架
- OpenVas 是使用 Nessus 2 為基礎發展的開放原始碼弱點掃描軟體。
- 目前提供了35,000 的弱點掃描資料庫。

OpenVAS 架構


OpenVAS
Open Vulnerability Assessment System
Scan Targets
OpenVAS CLI
Greenbone Security Assistant
Clients
OpenVAS Scanner
OpenVAS Manager
Services
NVT's
Results, Configs
Data

OpenVAS運作畫面





OpenVAS


Greenbone
Security Assistant
登录为 Admin admin | 注销
Tue Apr 12 03:08:59 2016 UTC
扫描管理
资产管理
SecInfo 管理
配置
附加功能
管理本软件
帮助
任务 (总计: 0)
√不自动刷新
过滤器:
apply_overrides=1 rows=10 first=1 sort=name
--
名称
状态
报告
总计
最后的
严重性
趋势
动作
√Apply to page contents
(应用的过滤器: apply_overrides=1 rows=10 first=1 sort=name)
(总计: 0)
亲，欢迎您!
为了探索这个强力的应用程序和首次来快速开始工作，我在这里辅助您一些提示和快捷操作。
我将自动出现在您没创建或创建了少量对象的地方，并且在您创建了多于 3 个对象的时候消失。您可以通过这个向导图标呼叫我 ，在以后任何时间都行。
快速开始：立即扫描一个 IP 地址
IP 地址或主机名：
开始扫描

查看掃描狀態

- 點選掃描管理 -> 報告 即可看到目前掃描目標主機的相關資訊 ，點選需要看的報告後即可看到詳細的內容

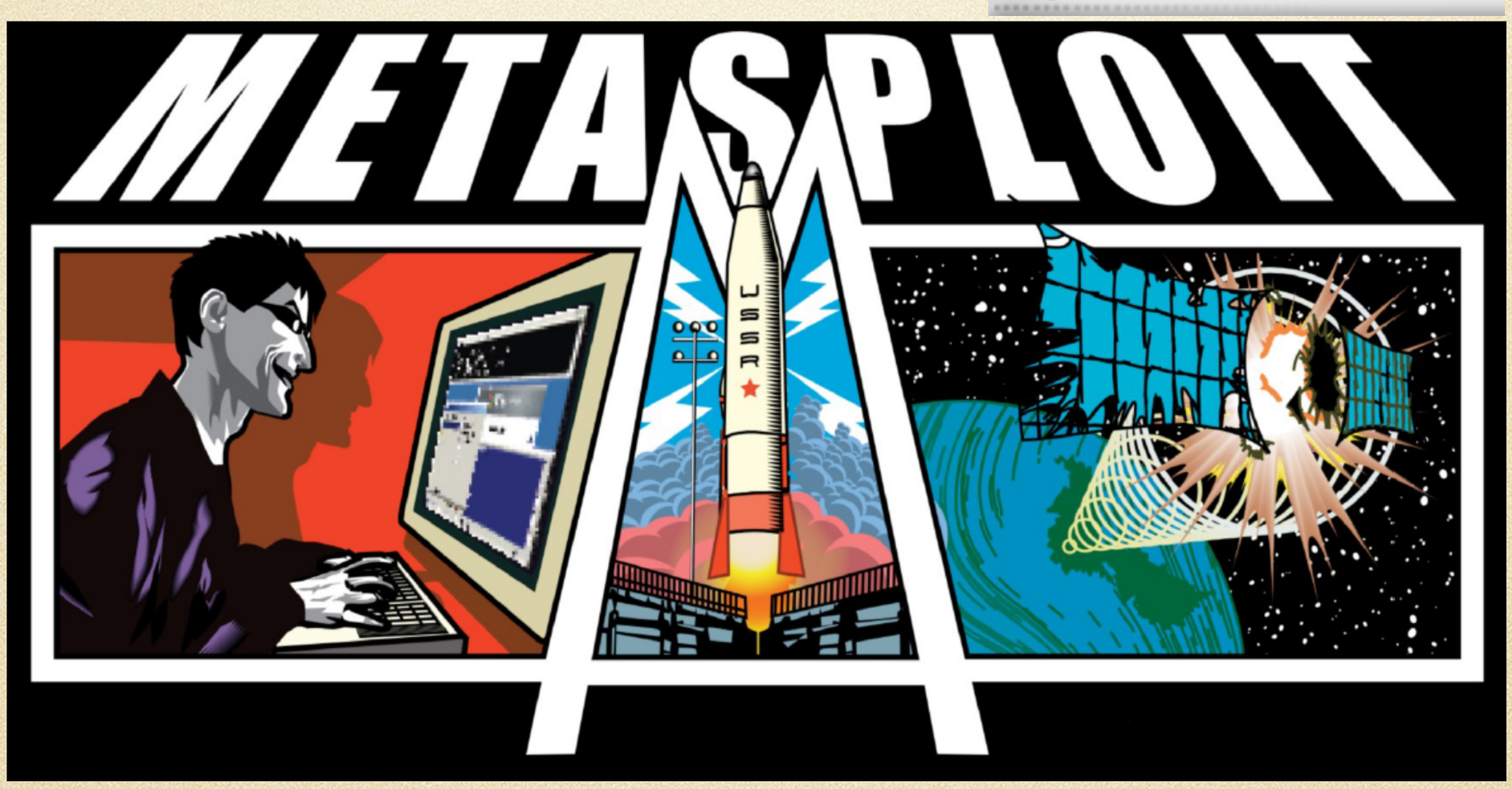
弱點掃描報告


Greenbone
Security Assistant
登录为 Admin admin | 注销
Tue Apr 12 03:26:22 2016 UTC
扫描管理
资产管理
SecInfo 管理
配置
附加功能
管理本软件
帮助
报告：结果 1 - 59 / 59 (总计: 84)
PDF
32 %
过滤器: sort-reverse=severity result_hosts_only=1 min_cvss_base= min_qod= le
漏洞
严重性
QoD
主机
位置
动作
X Server 10.0 (高) 75% 172.16.34.146 6000/tcp
PostgreSQL weak password 9.0 (高) 75% 172.16.34.146 5432/tcp
PostgreSQL Multiple Security Vulnerabilities 8.5 (高) 75% 172.16.34.146 5432/tcp
phpMyAdmin Code Injection and XSS Vulnerability 7.5 (高) 75% 172.16.34.146 80/tcp
phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities 7.5 (高) 75% 172.16.34.146 80/tcp
phpMyAdmin Configuration File PHP Code Injection Vulnerability 7.5 (高) 75% 172.16.34.146 80/tcp
phpinfo() output accessible 7.5 (高) 80% 172.16.34.146 80/tcp
PostgreSQL Multiple Security Vulnerabilities 6.8 (中) 75% 172.16.34.146 5432/tcp
PostgreSQL NULL Character CA SSL Certificate Validation Security Bypass Vulnerability 6.5 (中) 75% 172.16.34.146 5432/tcp
PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability 6.5 (中) 75% 172.16.34.146 5432/tcp
PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability 6.5 (中) 75% 172.16.34.146 5432/tcp
PostgreSQL PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability 6.0 (中) 75% 172.16.34.146 5432/tcp
PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability 5.5 (中) 75% 172.16.34.146 5432/tcp
phpMyAdmin Unspecified SQL Injection and Cross Site Scripting Vulnerabilities 4.3 (中) 75% 172.16.34.146 80/tcp
phpMyAdmin SQL bookmark XSS Vulnerability 4.3 (中) 75% 172.16.34.146 80/tcp

弱點掃描報告

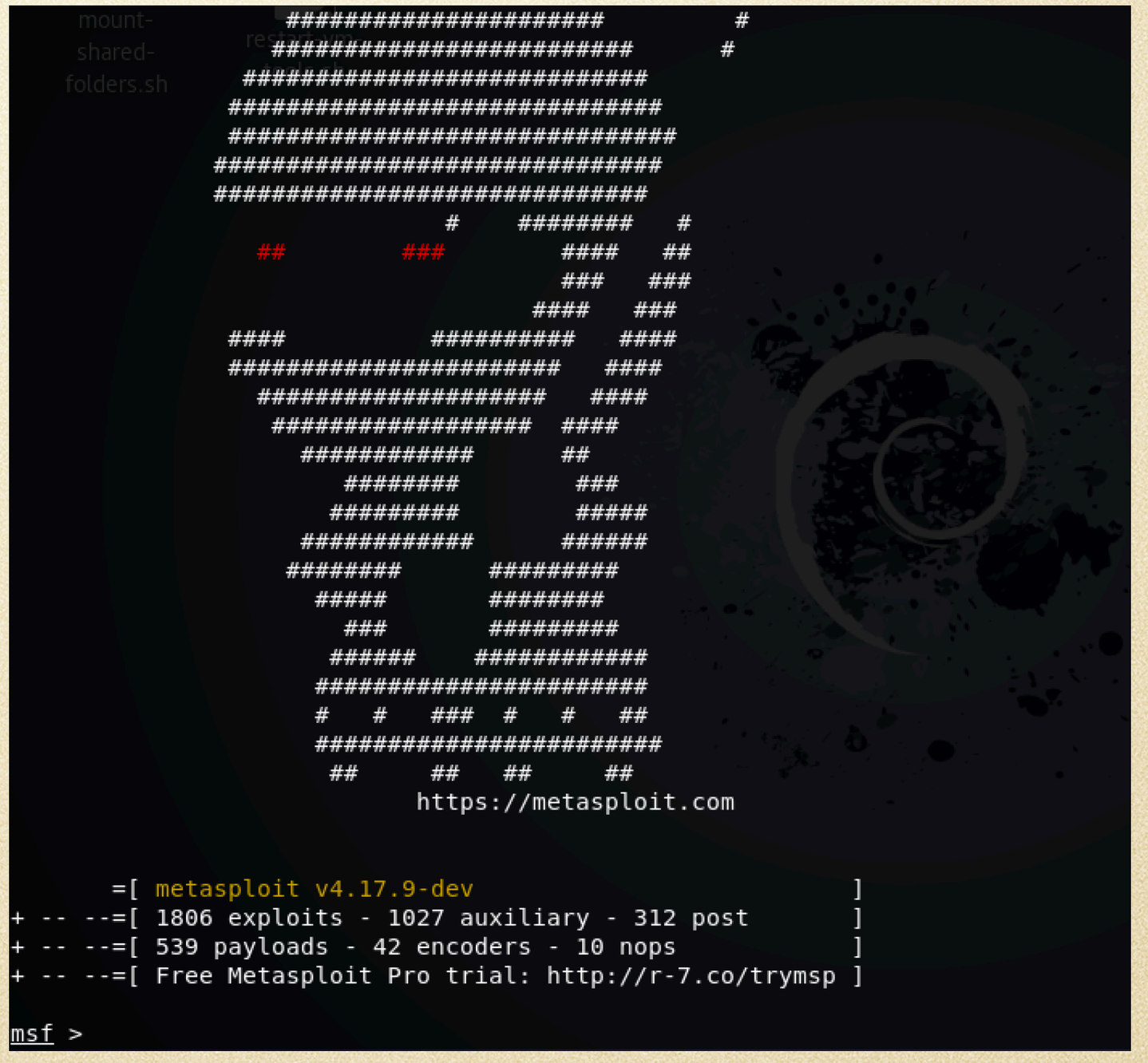

Greenbone
Security Assistant
登录为 Admin admin | 注销
Tue Apr 12 03:32:20 2016 UTC
扫描管理
资产管理
SecInfo 管理
配置
附加功能
管理本软件
帮助
结果详情
任务: Immediate scan of IP 172.16.34.146
ID: 6f82cee8-bf8a-4767-a020-9f1043e48ebb
漏洞
严重性
QoD
主机
位置
动作
PostgreSQL weak password
9.0 (高)
75%
172.16.34.146
5432/tcp
摘要
It was possible to login into the remote PostgreSQL as user postgres using weak credentials.
漏洞检测结果
It was possible to login as user postgres with password "postgres".
解决方案
Change the password as soon as possible.
漏洞的检测方法
详情: PostgreSQL weak password (OID: 1.3.6.1.4.1.25623.1.0.103552)
使用的版本: $Revision: 12 $

Metasploit Framework



啟動Metasploit

- #msfconsole



Metasploit Console Basic

- Search for module:
  - msf > search [regex]
- Specify and exploit to use:
  - msf > use exploit/[ExploitPath]
- Specify a Payload to use:
  - msf > set PAYLOAD [PayloadPath]

Metasploit Console Basic (cont.)

- Show options for the current modules:
  - msf > show options
- Set options:
  - msf > set [Option] [Value]
- Start exploit:
  - msf > exploit

```
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   GroomAllocations    12               yes       Initial number of times to groom the kernel pool.
   GroomDelta          5                yes       The amount to increase the groom count by per try.
   MaxExploitAttempts  3                yes       The number of times to retry the exploit.
   ProcessName         spoolsv.exe      yes       Process to inject payload into.
   Proxies                              no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST                                yes       The target address
   RPORT               445              yes       The target port (TCP)
   SMBDomain           .                no        (Optional) The Windows domain to use for authentication
   SMBPass                              no        (Optional) The password for the specified username
   SMBUser                              no        (Optional) The username to authenticate as
   VerifyArch          true             yes       Check if remote architecture matches exploit Target.
   VerifyTarget        true             yes       Check if remote OS matches exploit Target.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

關於防禦

是否有什麼好的防禦方法？

總結

- 系統與應用軟體可能因程式開發過程中的錯誤，造成弱點的產生
- 目前為網路的時代，瀏覽網路存有潛在的風險
- 系統弱點掃瞄與分析，須定期進行以降低遭受入侵攻擊的機會
- 系統登錄檔為系統功能的設定，可配合相關工具軟體進行檢測

Q & A