

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



- 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

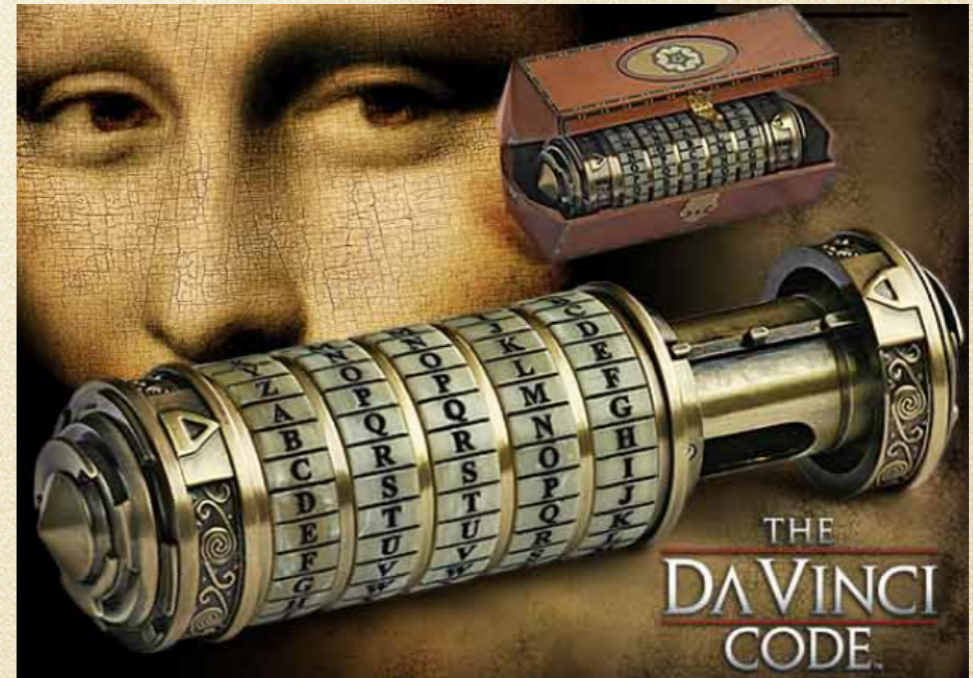
資訊安全十大領域

- 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

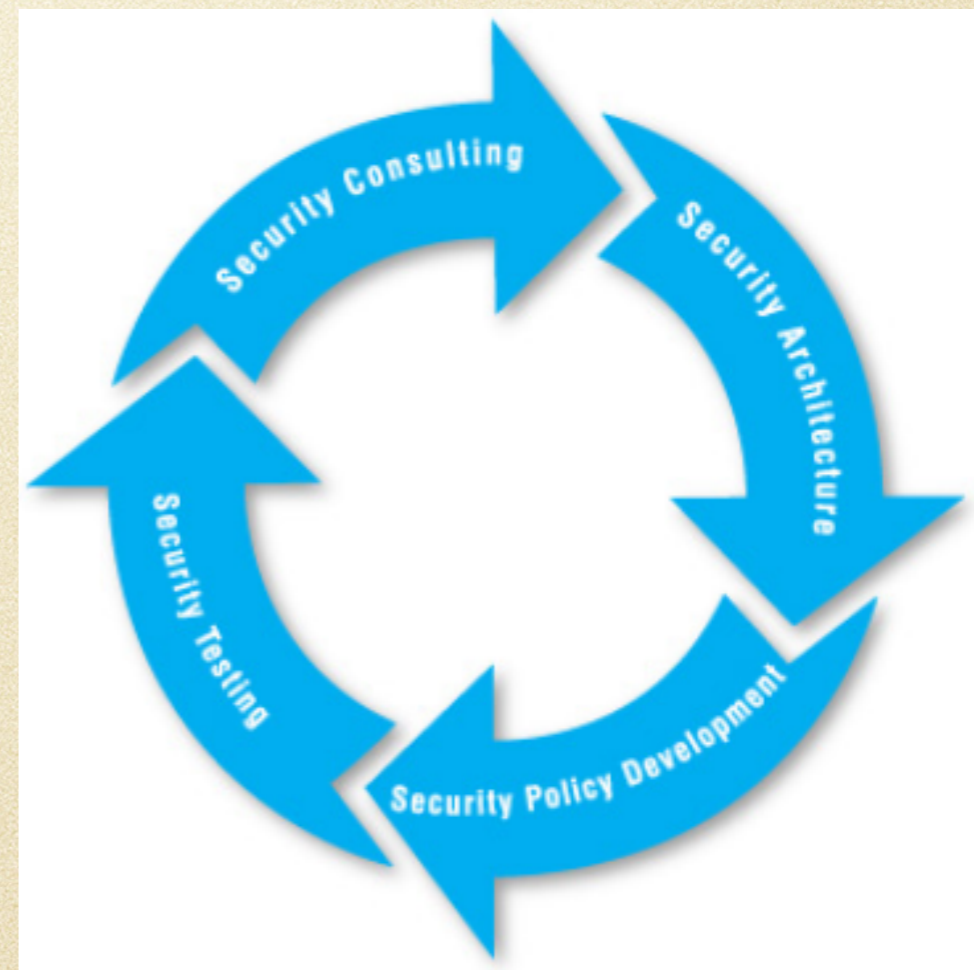
資訊安全十大領域

- 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



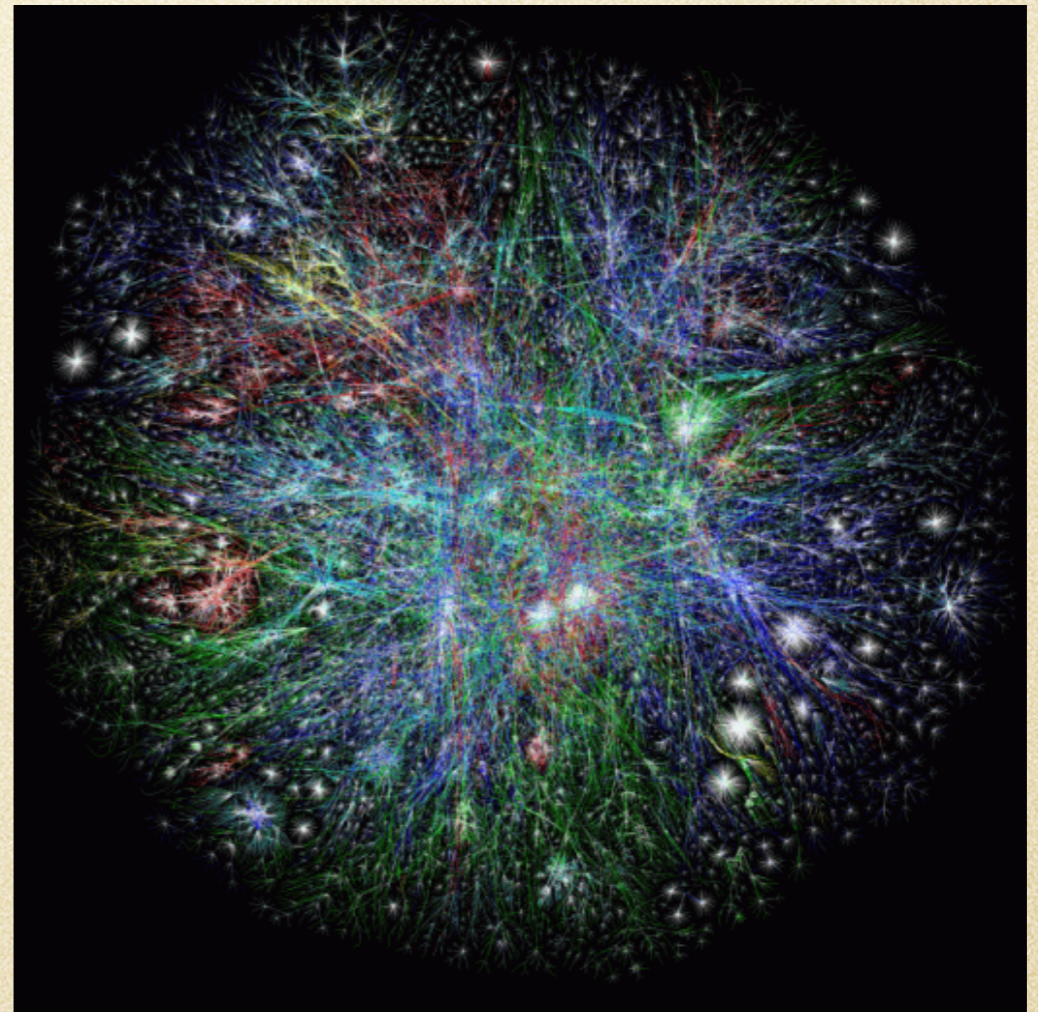
資訊安全十大領域

- 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



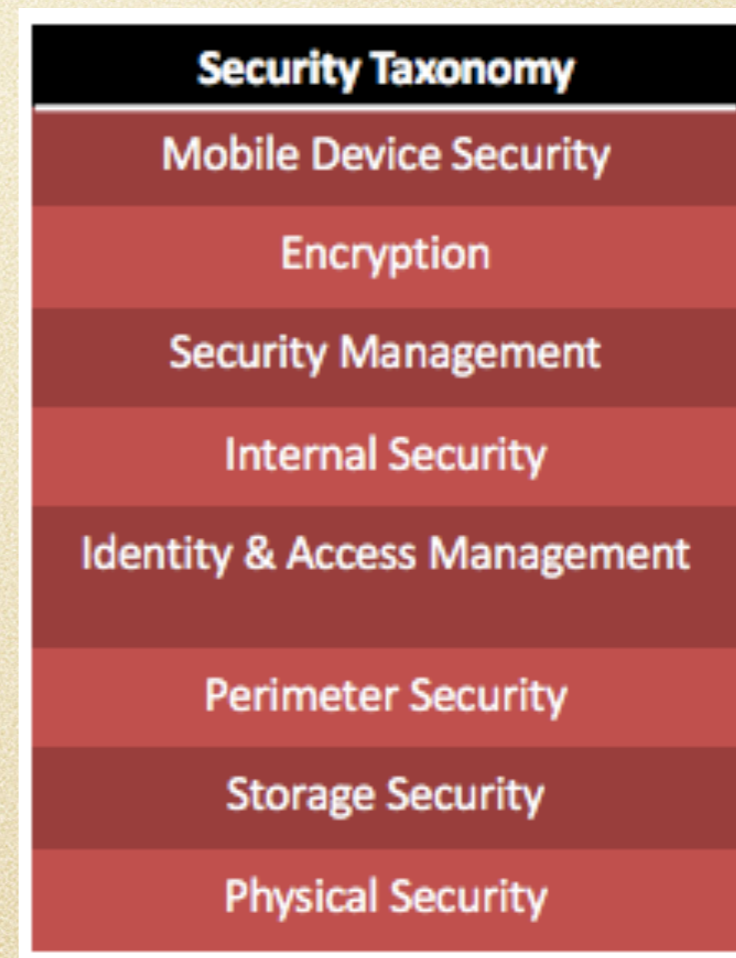
資訊安全十大領域

- 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

```
3732C20616E642070617463686513206F5590BF3  
76C6206C6974746C65 16E642074616C773192A  
A16C20Data BreachE2046520 1A07072216145A  
2E6F6163686573204C697474CC 520565CB74AF8  
Cyber Attack696EA1 486FAF64206 6E013921FC  
06564207368 206E61C F766 6C792Protection  
C6E207468652A261736B60142E20480810D3F5A8  
6368AF93010808B4FA017745C7A6 108B2C3FD55157  
0AFFA33C08E00F2A5697D011A56AFE64 0746865206  
02073 C732C20736852756B013A 0AA206336 5206  
16E642001A719System Safety Compromised1A7  
E00F2A5694C028BE5BF7D011A0010A3BCE561AF8701
```

如何進行

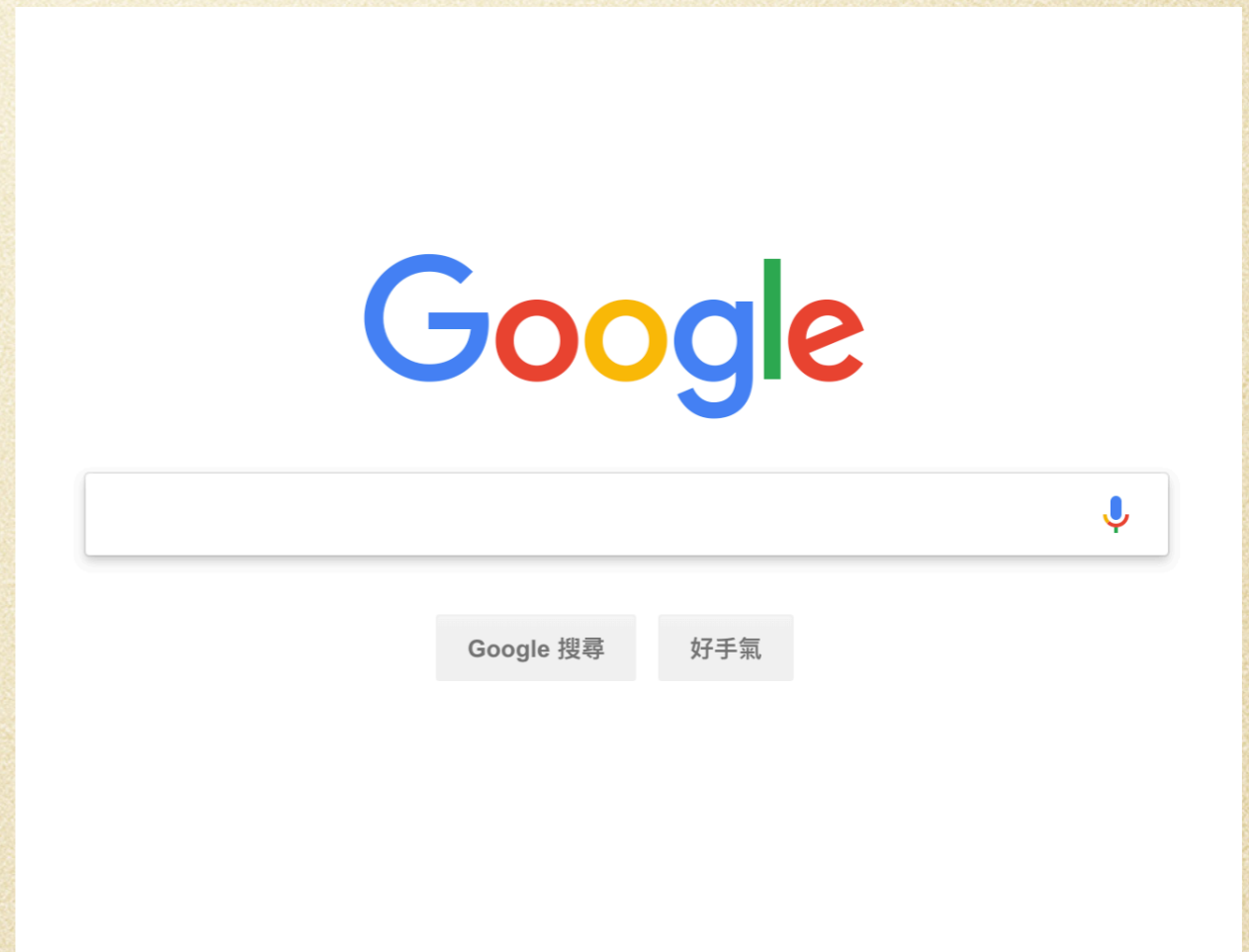
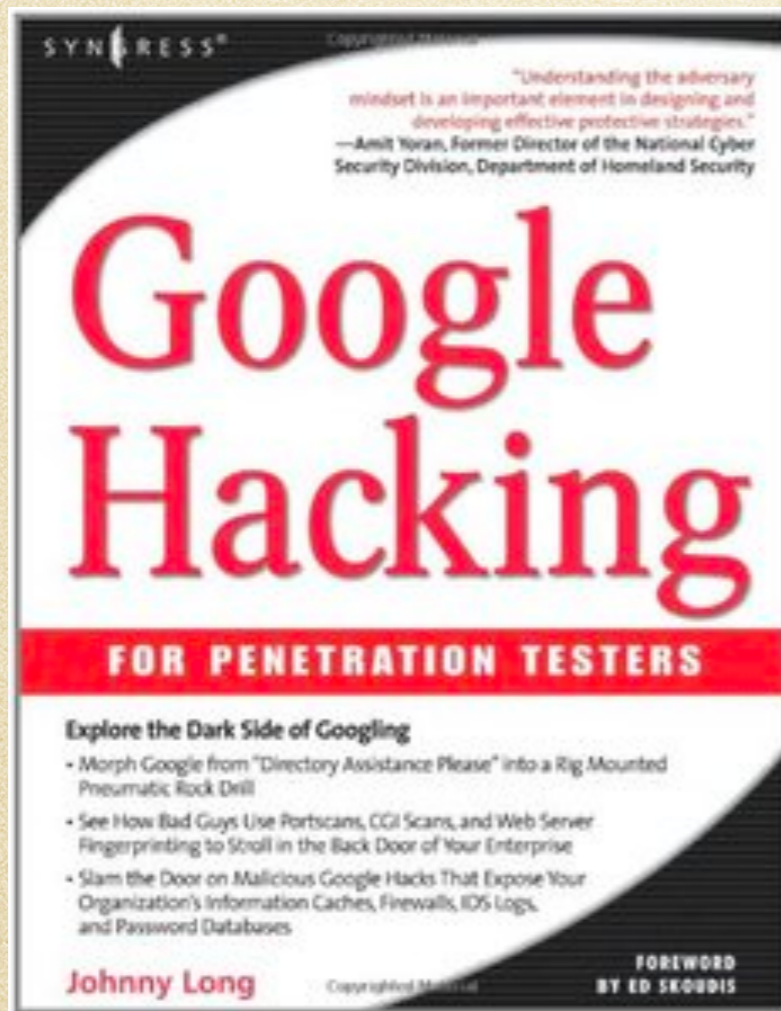
他們如何研究目標呢？

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



國家高速網路與計算中心
National Center for High-performance Computing
0800-351-510

傳真：
886-3-57

intitle



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

intext



台南分部

地址：



- 關於我們
- 組織架構
- 主任室
- 大事記要
- 交通與聯絡資訊
- 人才招聘
- 專利與技術轉移
- 參觀服務
- 場地租借
- 教育訓練
- 相關連結

尋找特定檔案
類型：filetype

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 CherrvFramework Themes 3.1.4 - Backun File Download	WebApps	PHP	h1n014r

https://www.exploit-db.com



Google Hacking Database

Show 15

Quick Search

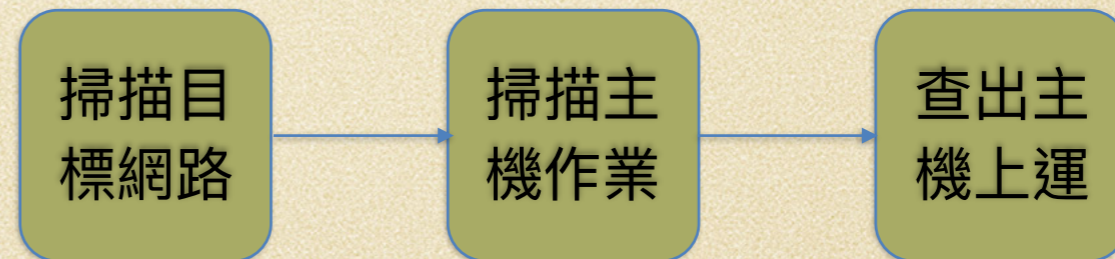
Date Added	Dork	Category	Author
2018-11-28	"inurl:"Umbraco/#/login" site:*edu"	Pages Containing Login Portals	CrimsonTorso
2018-11-28	"site:ghostbin.com " / " "	Files Containing Juicy Info	CrimsonTorso
2018-11-28	"site:hastebin.com " / " "	Files Containing Juicy Info	CrimsonTorso
2018-11-27	intitle:"index 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
2018-11-15	index of /skeditor	Sensitive Directories	ManhNho

[GHDB,https://www.exploit-db.com/google-hacking-database](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 (Port 21)、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

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

常見的通訊協定

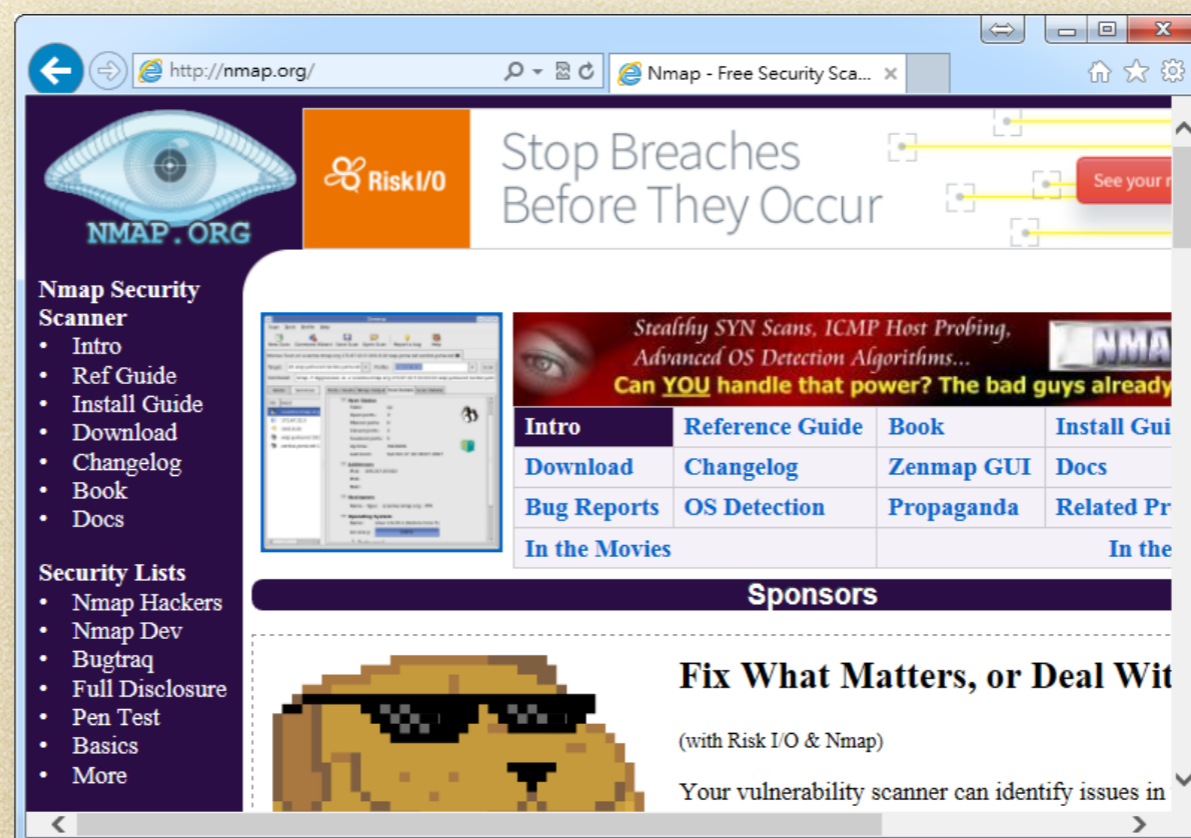
<i>PortNumber</i>	名稱	說明
115	<i>sftp</i>	安全的檔案傳輸協定
123	<i>ntp</i>	網路時間協定
137	<i>netbios-ns</i>	<i>netbios</i> 名稱服務
138	<i>netbios-dgm</i>	<i>netbios</i> 資料包服務
139	<i>netbios-dgm</i>	<i>netbios</i> 工作階段服務
143	<i>imap</i>	網際網路訊息存取協定
443	<i>https</i>	<i>https</i>
445	<i>microsoft-ds</i>	透過 <i>tcp/ip</i>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

常見的通訊協定

<i>PortNumber</i>	名稱	說明
3306	<i>mysql</i>	<i>mysql server</i>
3389	<i>rdp</i>	<i>windows</i> 遠端桌面
8080	<i>http</i>	<i>www</i> 服務
8443	<i>https</i>	<i>https</i>

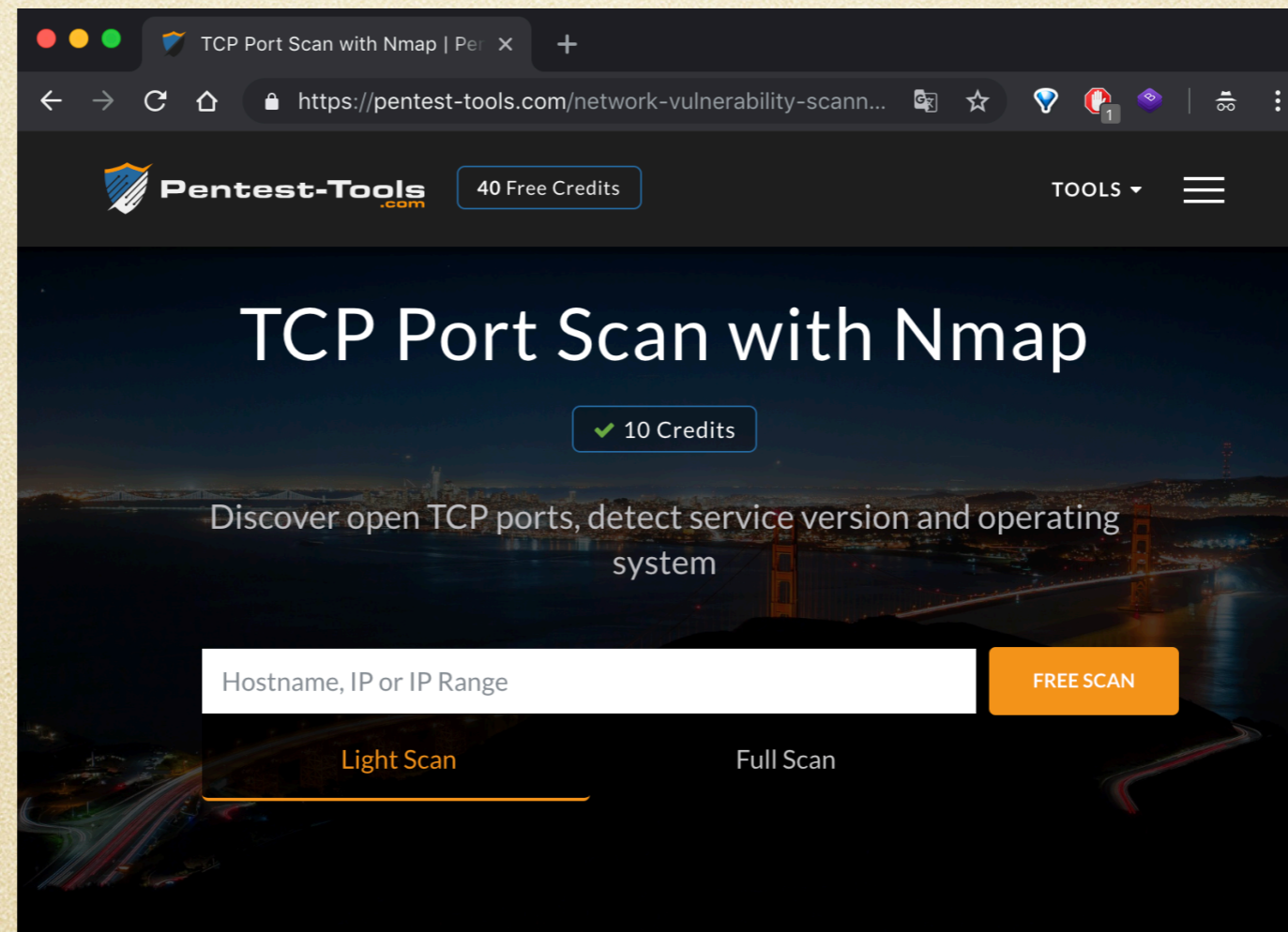
網路與主機掃瞄-Nmap

- 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



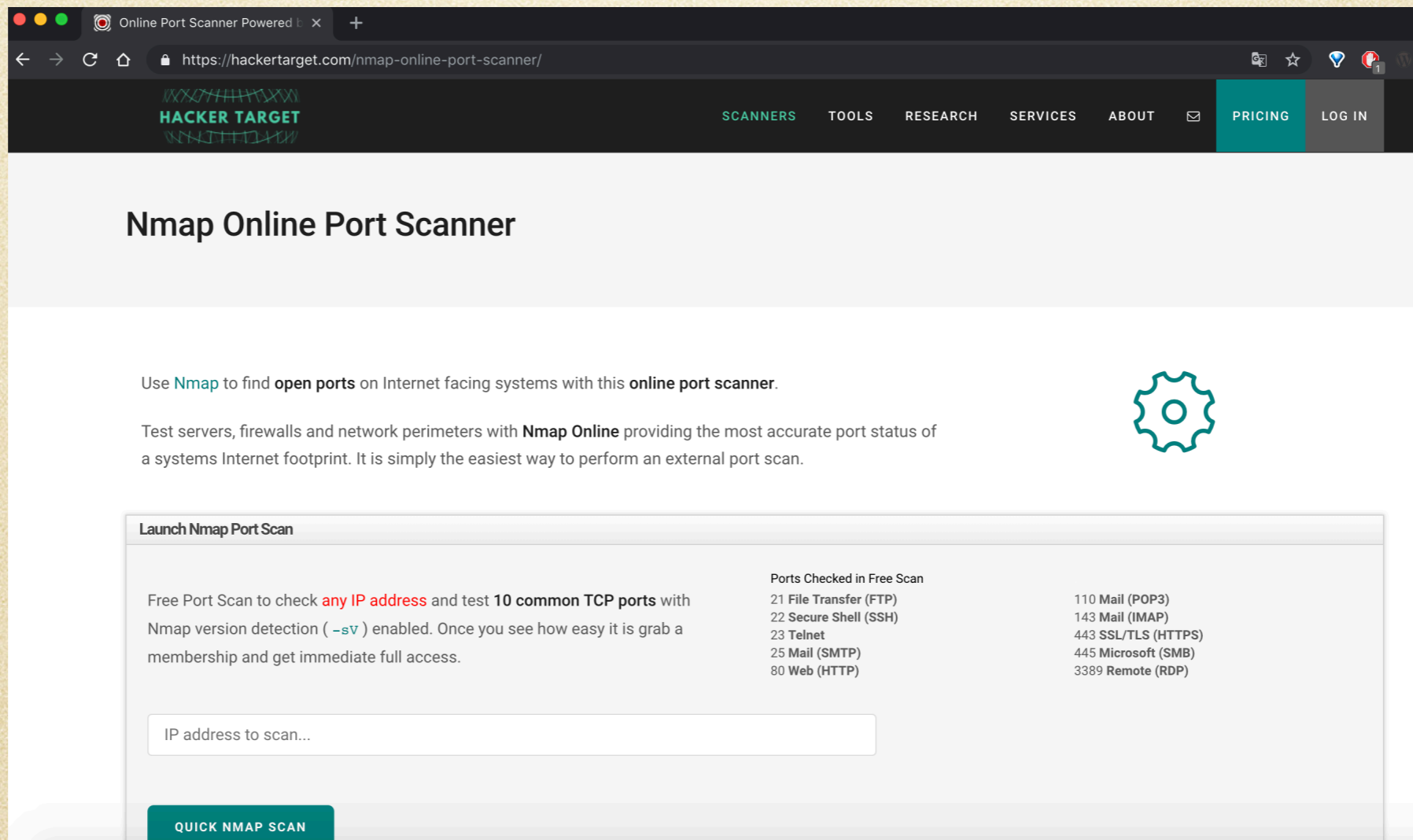
Online tools (1/2)

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



Online tools (2/2)

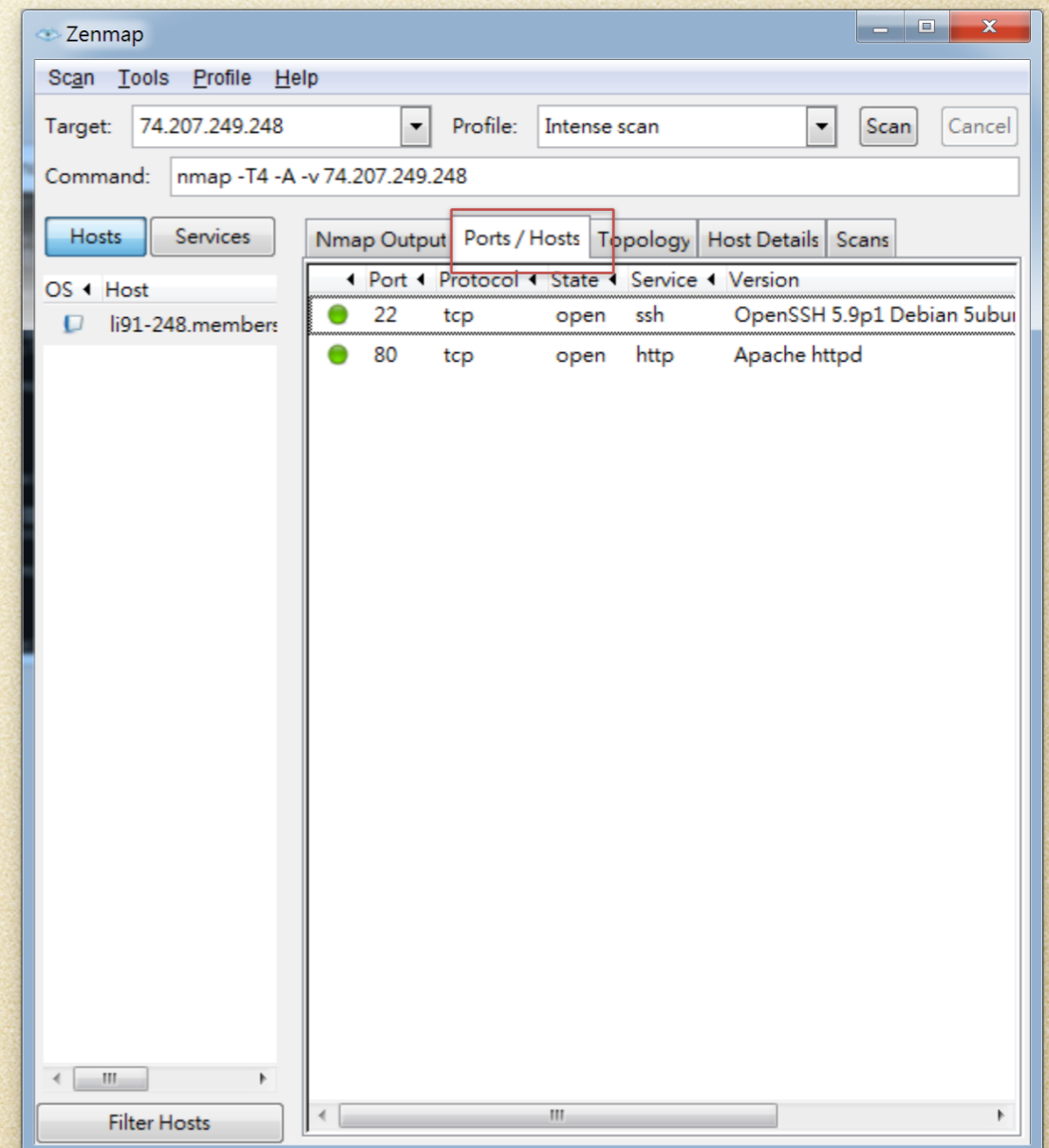
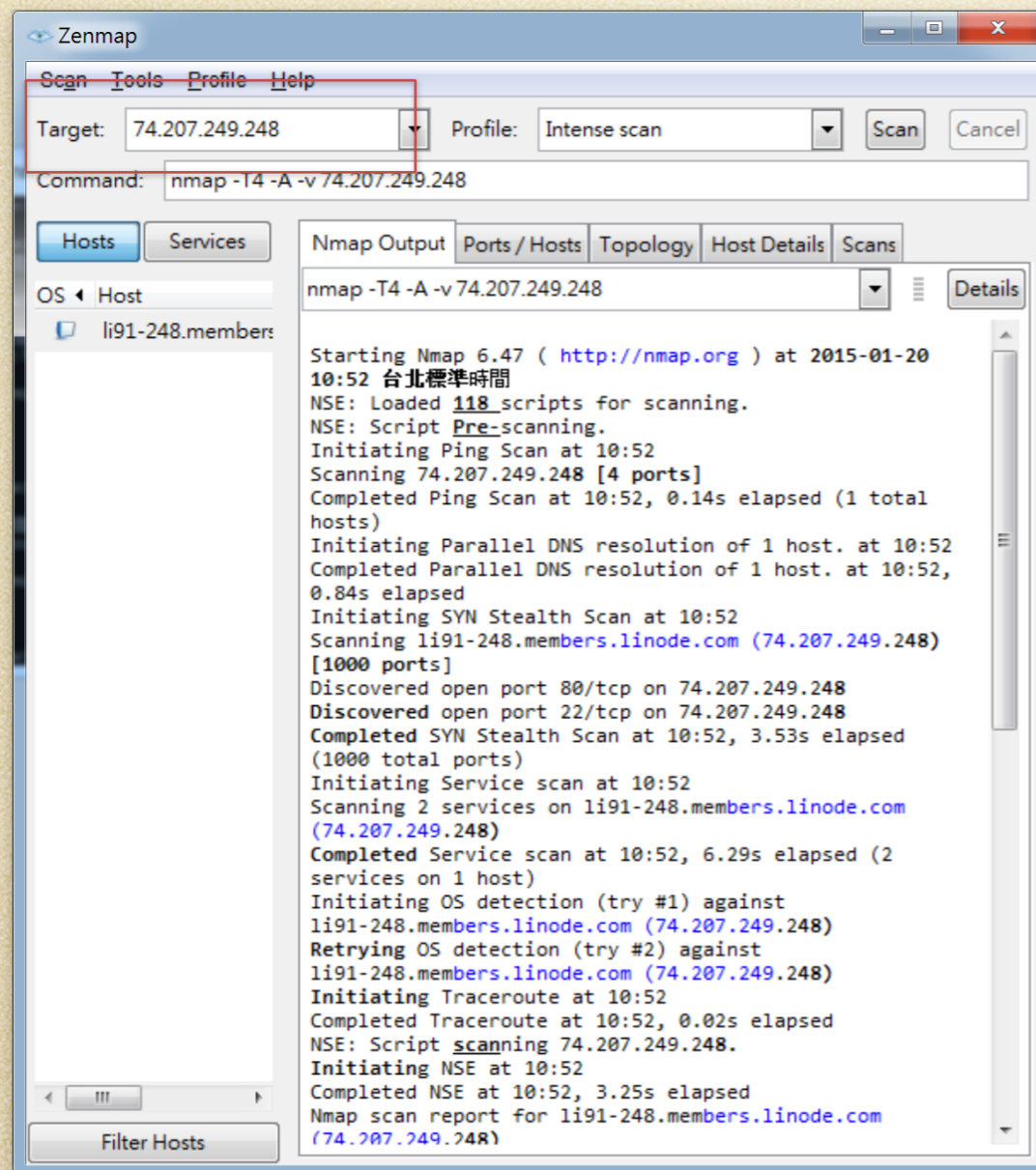
- <https://hackertarget.com/nmap-online-port-scanner/>



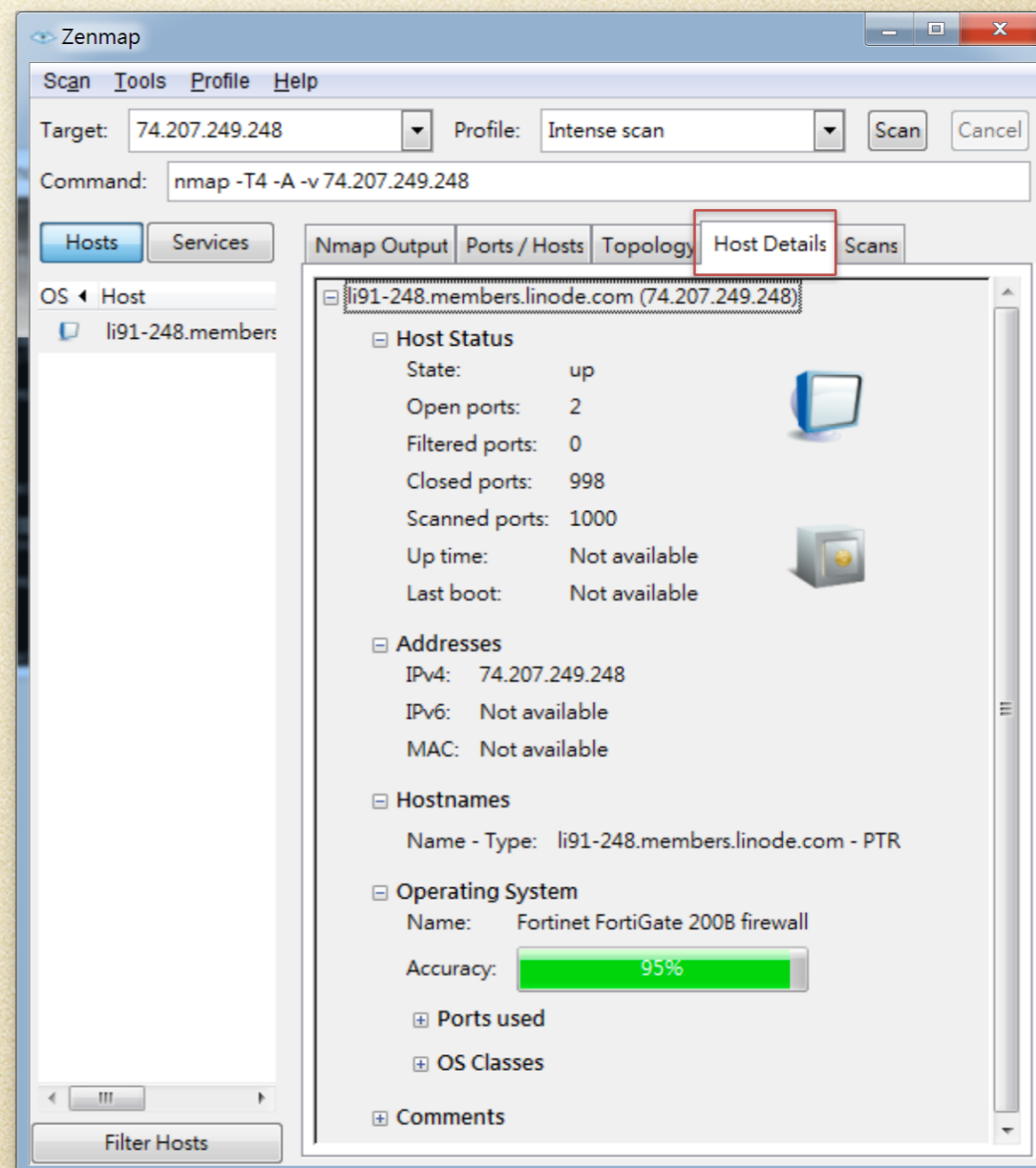
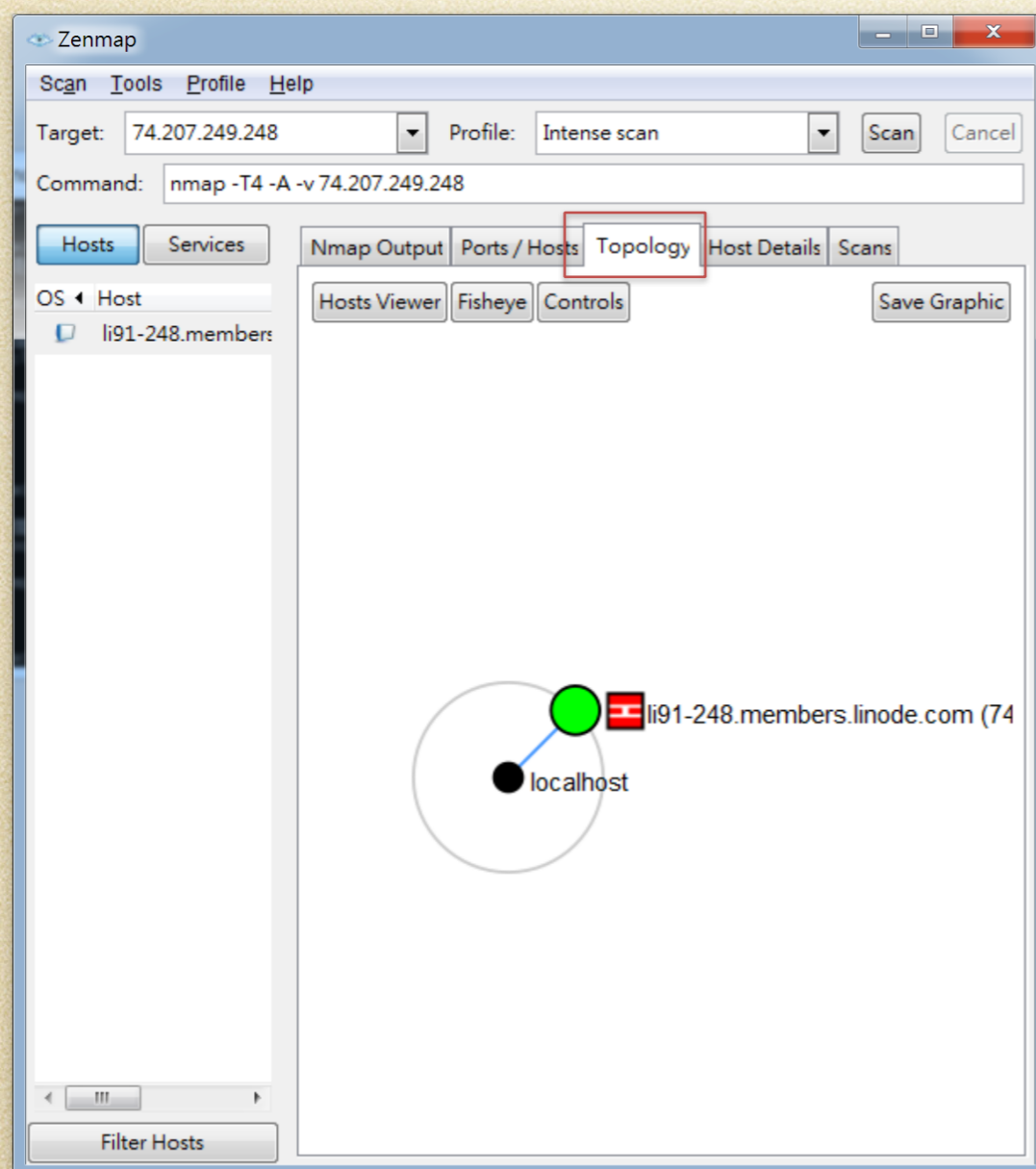
The screenshot shows a web browser window with the URL <https://hackertarget.com/nmap-online-port-scanner/>. The page features a dark navigation bar with the 'HACKER TARGET' logo and menu items: SCANNERS, TOOLS, RESEARCH, SERVICES, ABOUT, PRICING, and LOG IN. The main heading is 'Nmap Online Port Scanner'. Below this, there is a description: 'Use Nmap to find open ports on Internet facing systems with this online port scanner.' and 'Test servers, firewalls and network perimeters with Nmap Online providing the most accurate port status of a systems Internet footprint. It is simply the easiest way to perform an external port scan.' A gear icon is positioned to the right of this text. The 'Launch Nmap Port Scan' section contains a text box for 'IP address to scan...' and a 'QUICK NMAP SCAN' button. To the right of the text box, a list of 'Ports Checked in Free Scan' is displayed:

21 File Transfer (FTP)	110 Mail (POP3)
22 Secure Shell (SSH)	143 Mail (IMAP)
23 Telnet	443 SSL/TLS (HTTPS)
25 Mail (SMTP)	445 Microsoft (SMB)
80 Web (HTTP)	3389 Remote (RDP)

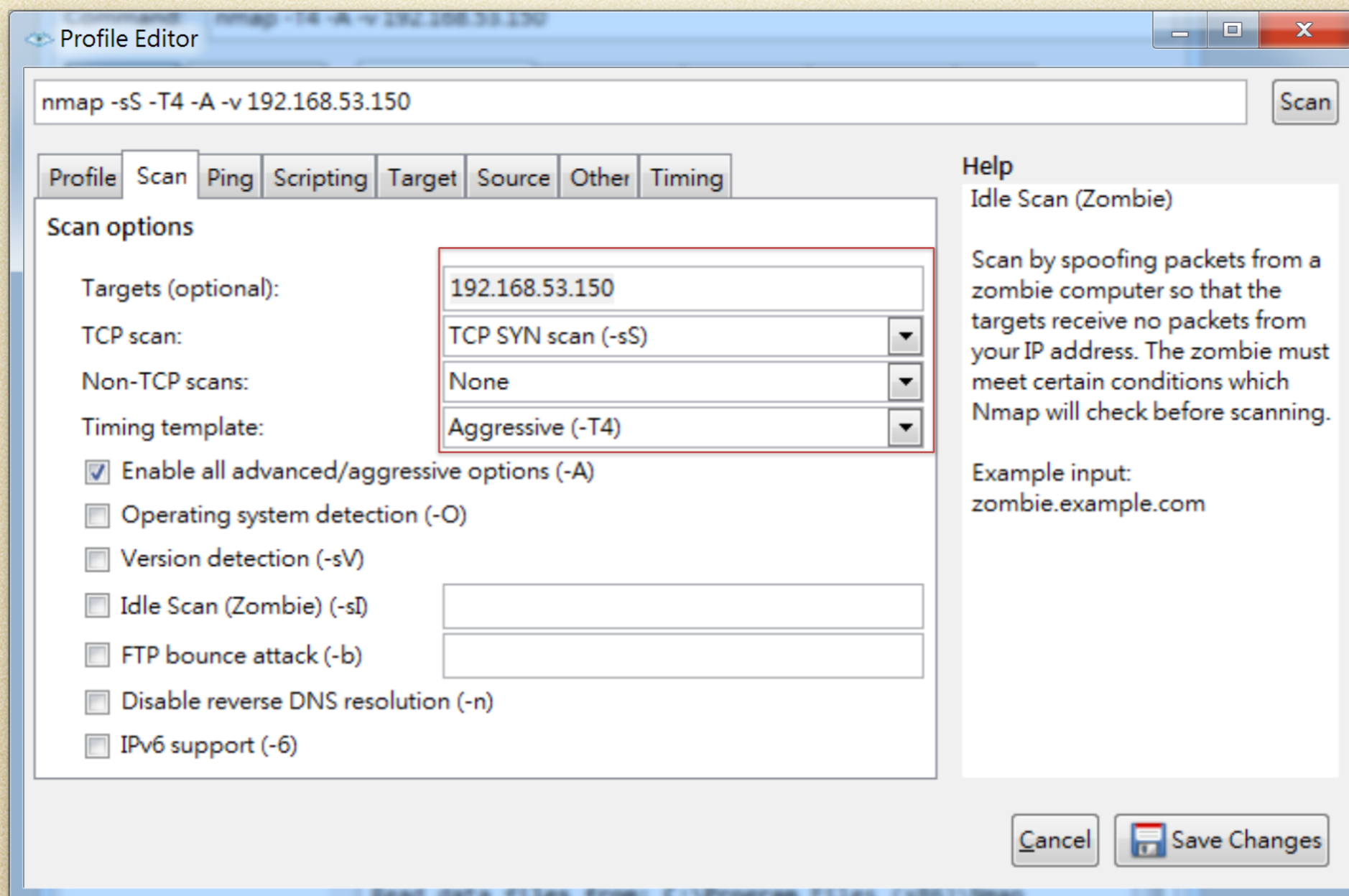
網路與主機掃瞄-Nmap



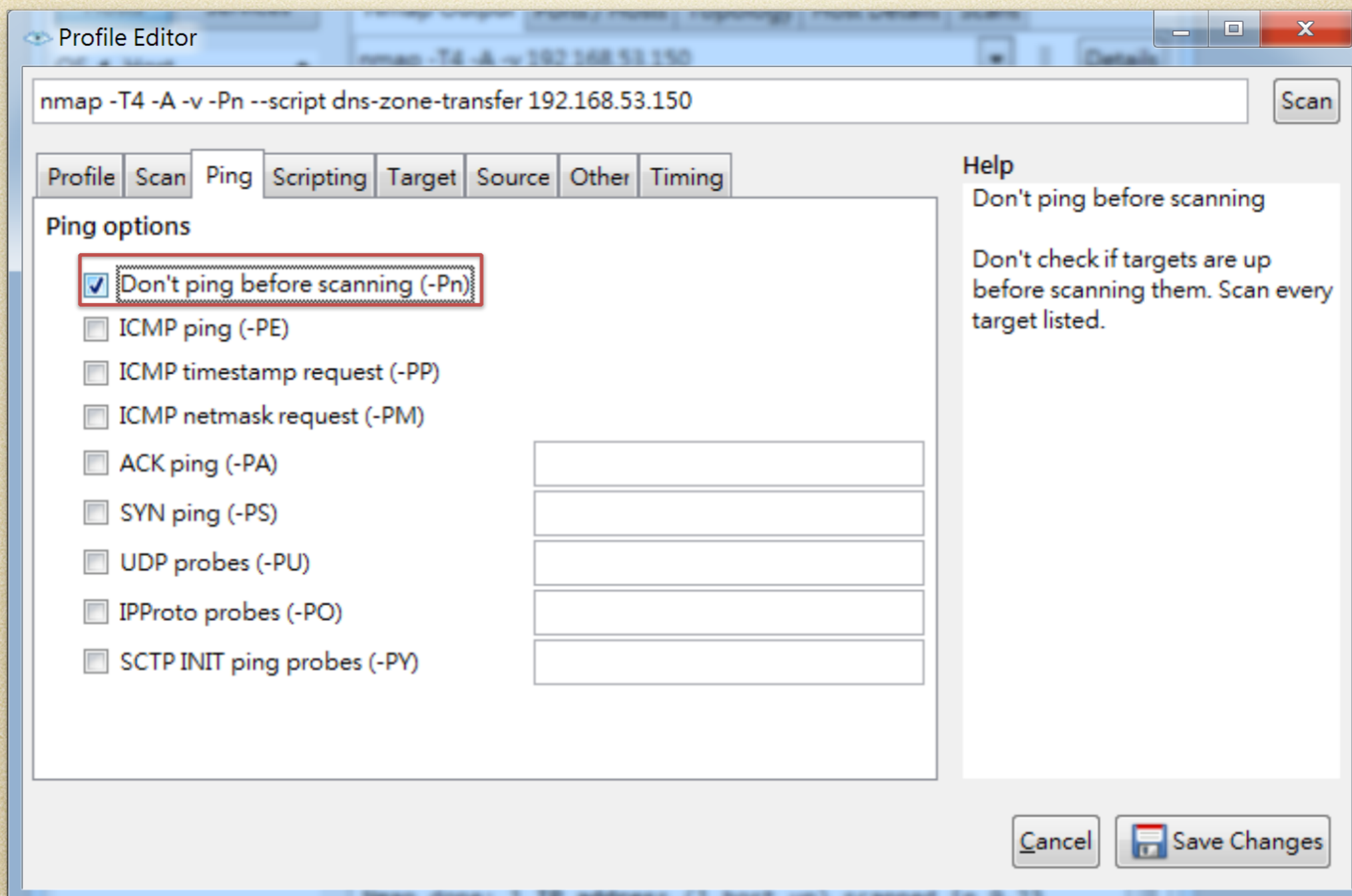
網路與主機掃瞄-Nmap



網路與主機掃瞄-Nmap

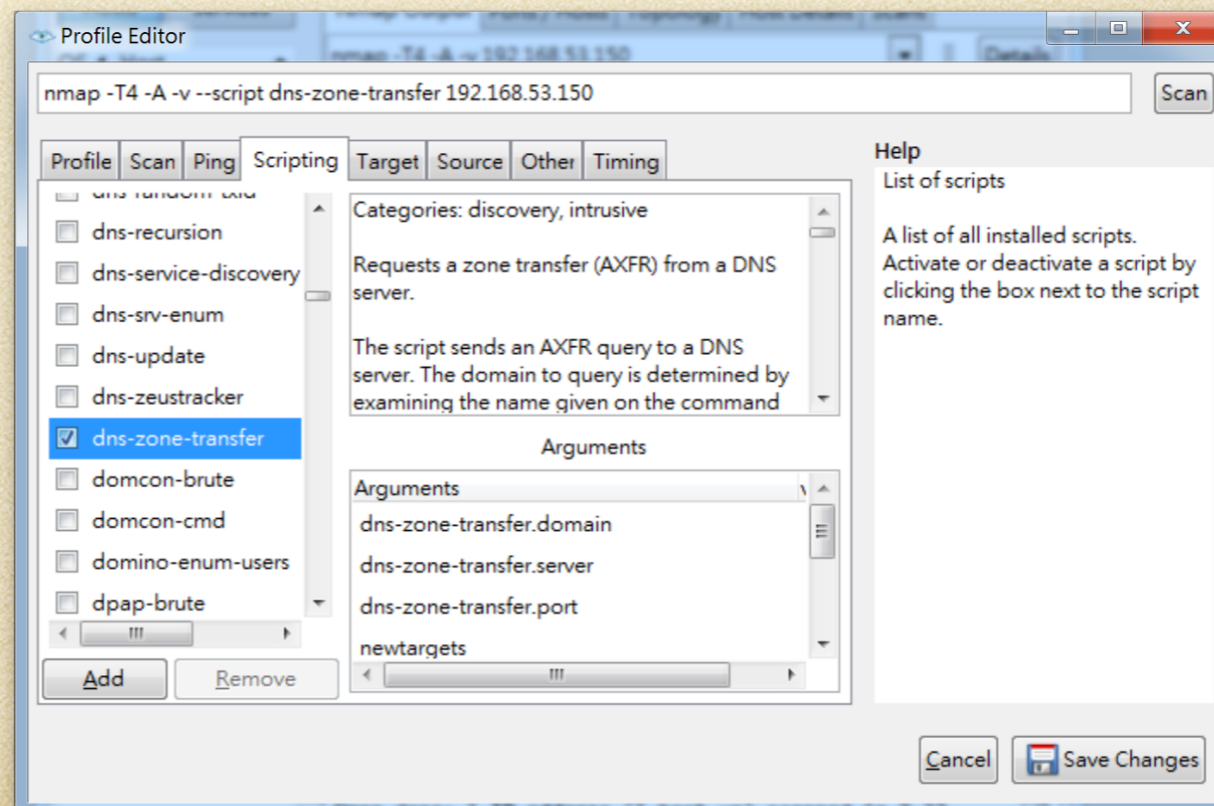


網路與主機掃瞄-Nmap



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



Fingbox

Partner

Support

Blog

[BUY NOW](#)

Web App

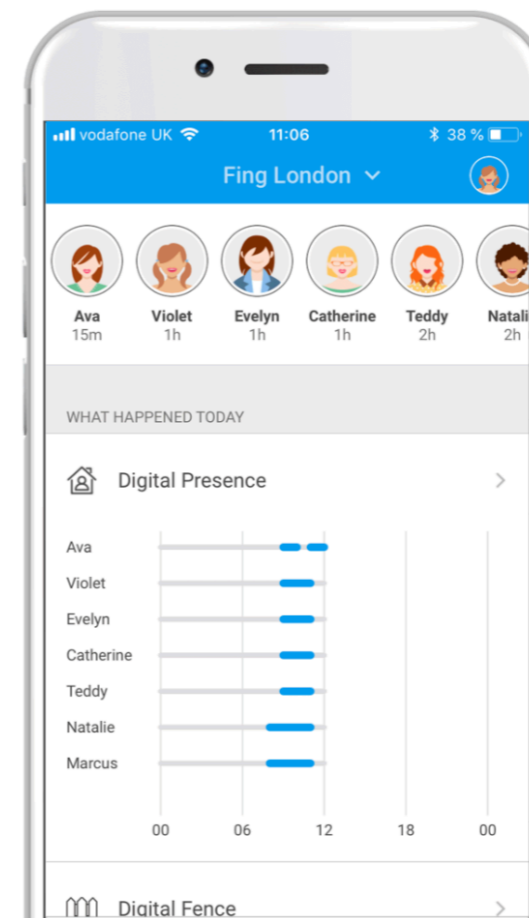
Troubleshoot and secure your home network with the Fing app and Fingbox sensor.

Download the free app today.

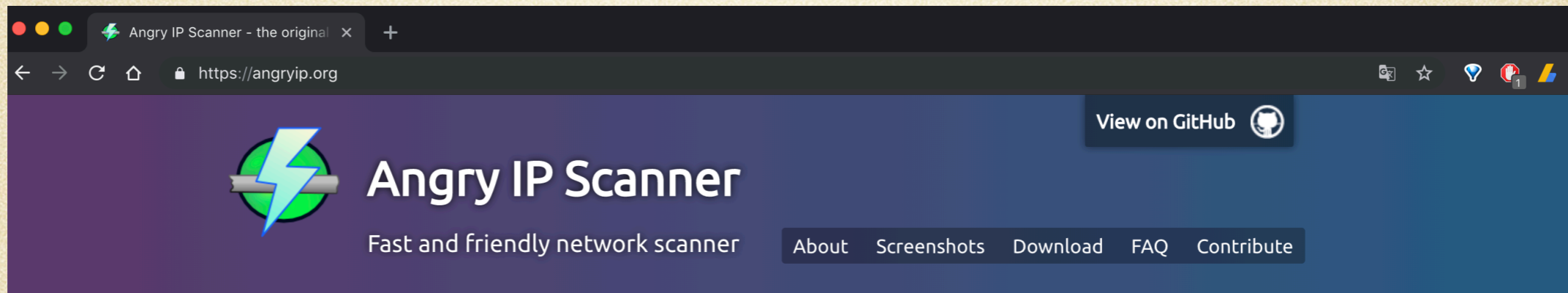


[Buy Fingbox](#)

[Learn More](#)



Angry IP

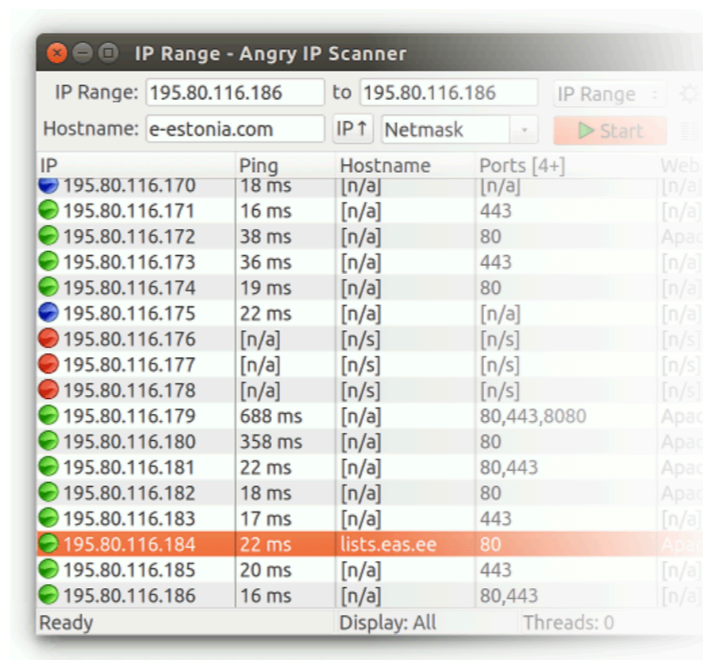


Features

- 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](#)



IP	Ping	Hostname	Ports [4+]	Web d
195.80.116.170	18 ms	[n/a]	[n/a]	[n/a]
195.80.116.171	16 ms	[n/a]	443	[n/a]
195.80.116.172	38 ms	[n/a]	80	Apache
195.80.116.173	36 ms	[n/a]	443	[n/a]
195.80.116.174	19 ms	[n/a]	80	[n/a]
195.80.116.175	22 ms	[n/a]	[n/a]	[n/a]
195.80.116.176	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.177	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.178	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.179	688 ms	[n/a]	80,443,8080	Apache
195.80.116.180	358 ms	[n/a]	80	Apache
195.80.116.181	22 ms	[n/a]	80,443	Apache
195.80.116.182	18 ms	[n/a]	80	Apache
195.80.116.183	17 ms	[n/a]	443	[n/a]
195.80.116.184	22 ms	lists.eas.ee	80	Apache
195.80.116.185	20 ms	[n/a]	443	[n/a]
195.80.116.186	16 ms	[n/a]	80,443	[n/a]

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

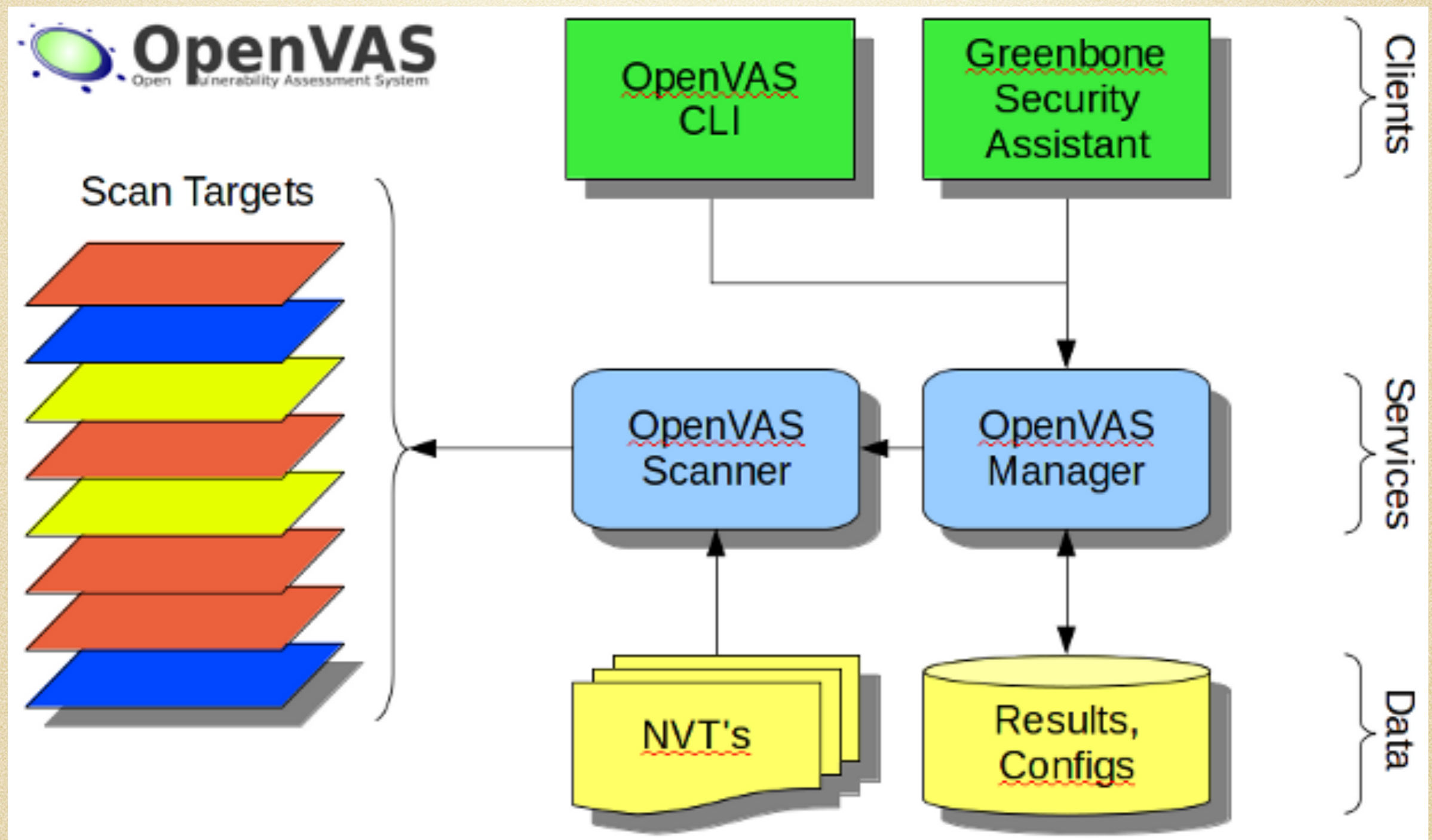
- 針對系統服務的弱點評估
 - Nessus(<http://www.tenable.com/products/nessus>)
 - Openvas (<http://www.openvas.org/>)
- 針對Web 應用程式的弱點評估
 - O-scan (<http://www.wesoft.info/download.php>)
 - Vega (<https://subgraph.com/vega/>)
 - W3af(<http://w3af.org/>)

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 運作畫面

Greenbone Security Assistant - Namoroka

File Edit View History Bookmarks Tools Help

192.168.11.93 https://192.168.11.93/omp?cmd=get_tasks&overrides=

Greenbone Security Assistant

Logged in as demo | Logout

Fri Oct 1 11:57:31 2010 (UTC)

Navigation

- Scan Management
 - Tasks
 - New Task
 - Notes
 - Overrides
 - Performance
- Configuration
 - Scan Configs
 - Targets
 - Credentials
 - Agents
 - Escalators
 - Schedules
- Administration
 - Users
 - NVT Feed
 - Settings
- Help
 - Contents
 - About

Tasks ? * [No auto-refresh] [Apply overrides]

Task	Status	Reports		Threat	Trend	Actions
		Total	Last			
Conficker Search (Search for Conficker on our Windows machines.)	Done	2	Jun 15 2010	None		
Deep Scan Linux (This does a deep scan of our GNU/Linux lab machine.)	Stopped at 23 %	0				
Deep Scan Windows (This does a deep scan of our Microsoft Windows lab machine.)	0 %	1				
IT-Grundsutz Scan (Tests for Compliance with IT-Grundsutz, 11. EL)	Done	2				
Nightly Scan (This scan does a nightly scan of the entire network and sends a mail if the threat level increases.)	Done	51				
Quick Scan Linux (This does a quick scan of our GNU/Linux lab machine.)	Paused at 98 %	2				

Greenbone Security Assistant (GSA) Copyright 2009

Greenbone Security Desktop

File Task View Settings Extras Help

Dashboard

Vulnerabilities: High: 106, Medium: 27, Low: 47

Scan Tasks: High: 2, Medium: 2, Low: 1, None: 1

Top 5 Tasks: Deep Scan Windows: 10, Conficker Search: 1, Nightly Scan: 1, Quick Scan Linux: 1, IT-Grundsutz Scan: 8

System Load: 1 min: 0.00 Min, 0.18 Avg, 1.01 Max, 0.99 Last; 5 min: 0.00 Min, 0.17 Avg, 0.46 Max, 0.15 Last; 15 min: 0.00 Min, 0.13 Avg, 0.30 Max, 0.13 Last

Trends: 0, 0, 0, 0, 4

Task Overview: Total: 6, Running: 0, Progress: 1, Done: 5, New: 0, Error: 0

Resources Overview: Targets: 14, Scan Configs: 8, Schedules: 1, Escalators: 2, Credentials: 2, Agents: 0, Overrides: 0, Notes: 0

Tasks

Name	Status	Reports	First	Last	Threat	Trend
Quick Scan Linux	Done	2	Jun 15 2010	Jun 15 2010	Medium	
Conficker Search	Done	1	Jun 15 2010	Jun 15 2010	High	
IT-Grundsutz Scan	Done	1	Jun 15 2010	Jun 15 2010	Low	
Deep Scan Linux	Stopped at 23%	0			None	
Nightly Scan	Done	102	Jun 16 2010	Apr 5 2011	Medium	
Deep Scan Windows	Done	10	Jun 15 2010	Jun 15 2010	High	

Report Deep Scan Windows (Tue Jun 15 09:12:22 2010)

Results 1 - 100 of 130

High (CVSS: 9.3)
NVT: Microsoft Windows Indeo Codec Multiple Vulnerabilities (OID: 1.3.6.1.4.1.25623)

Overview: This host is installed with Microsoft Windows Indeo codec and pr...
Multiple Vulnerability
Vulnerability Insight:
The multiple flaws are due to:
- An error in the Indeo4l codec when processing a specific size within the 'movi' record of a IV4l stream can be exploited to cause a heap-based bu...
- An error in the Indeo4l codec when decompressing a video stream can be exploited to cause a stack-based buffer overflow.

OpenVAS

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		严重性	趋势	动作
		总计	最后的			

√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!
为了探索这个强大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：

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


The screenshot shows the Greenbone Security Assistant interface. The top navigation bar includes '扫描管理' (Scanning Management), '资产管理' (Asset Management), 'SecInfo 管理' (SecInfo Management), '配置' (Configuration), '附加功能' (Additional Features), '管理本软件' (Manage This Software), and '帮助' (Help). The '扫描管理' menu is expanded, showing '任务' (Tasks), '报告' (Reports), '结果' (Results), '批注' (Comments), and '覆盖' (Overrides). The '报告' section is active, displaying a table with columns: '名称' (Name), '状态' (Status), '报告' (Reports), '严重性' (Severity), '趋势' (Trend), and '动作' (Action). The '报告' column is further divided into '总计' (Total) and '最后的' (Last). A single entry is visible: 'Immediate scan of IP 172.16.34.146' with a status of 32% and 0 reports.

名称	状态	报告		严重性	趋势	动作
		总计	最后的			
Immediate scan of IP 172.16.34.146	32 %	0 (1)				

The screenshot shows the Greenbone Security Assistant interface with the '报告' (Reports) section selected. The top navigation bar is the same as in the previous screenshot. The '报告' section is active, displaying a table with columns: '日期' (Date), '状态' (Status), '任务' (Task), '严重性' (Severity), '扫描结果' (Scan Results), and '动作' (Action). The '扫描结果' column is further divided into '高' (High), '中' (Medium), '低' (Low), '记录' (Records), and '假阳性' (False Positives). A single entry is visible: 'Tue Apr 12 03:16:42 2016' with a status of 32%, task 'Immediate scan of IP 172.16.34.146', severity of 10.0 (High), and scan results of 7 High, 10 Medium, and 3 Low.

日期	状态	任务	严重性	扫描结果					动作
				高	中	低	记录	假阳性	
Tue Apr 12 03:16:42 2016	32 %	Immediate scan of IP 172.16.34.146	10.0 (高)	7	10	3	39	0	

弱点扫描报告


























 **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

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 ? [menu] [down]

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	🔍 🌟

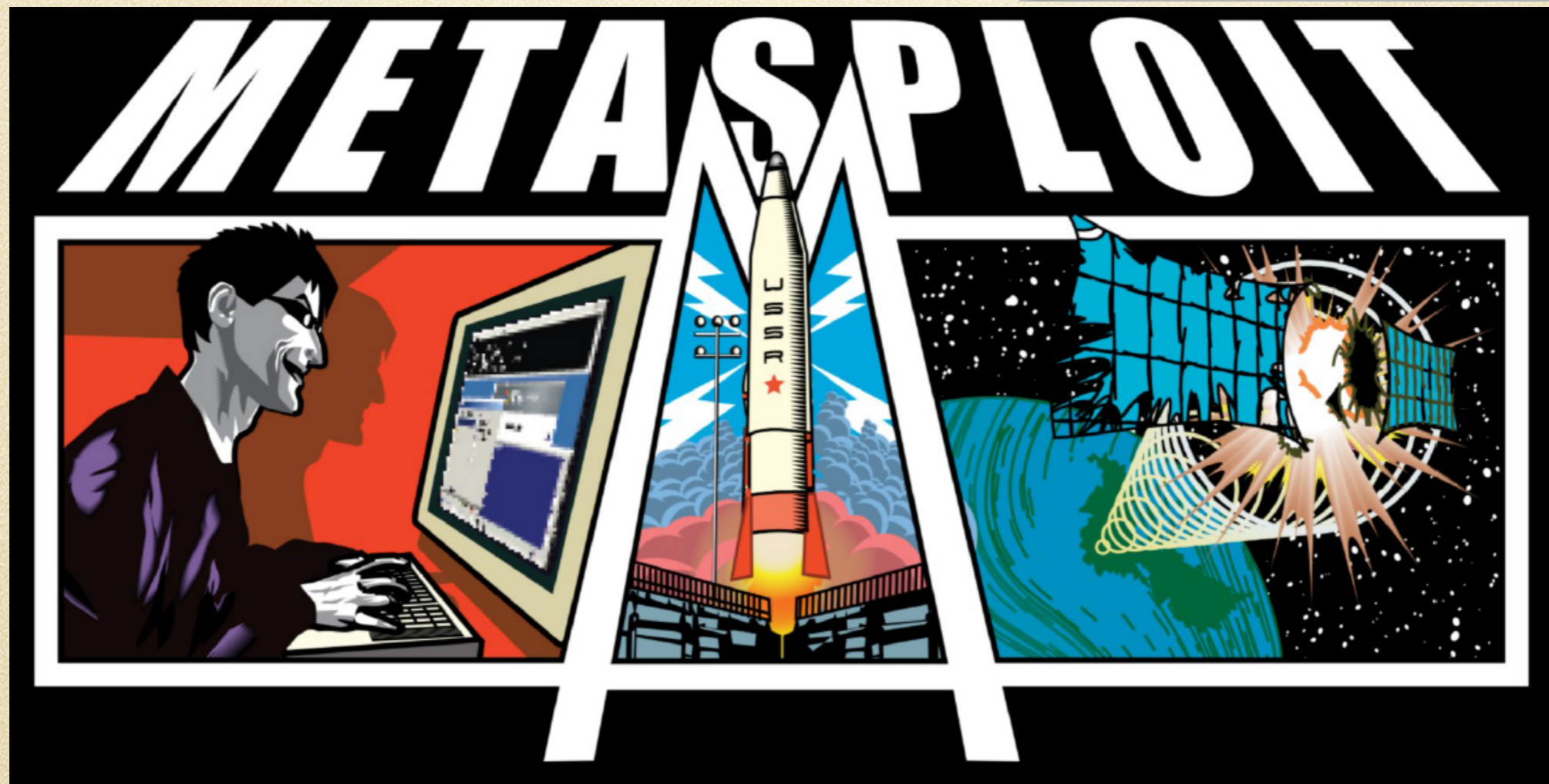
摘要
It was possible to login into the remote PostgreSQL as user postgres using weak credentials.

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



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
- 系統弱點掃描與分析，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

