弱點掃描與檢測實務

微智安聯

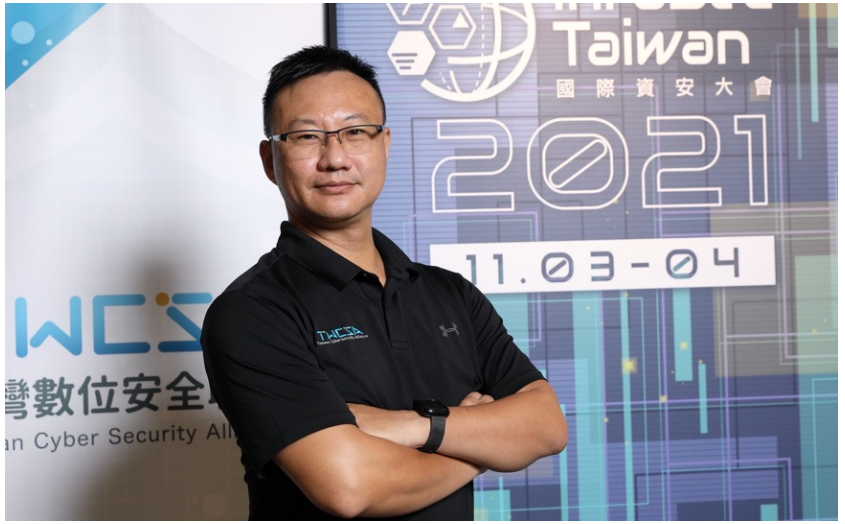
蔡一郎 執行長

SHIELDXTREME

Google Me.

現任

- ✓ 微智安聯股份有限公司 創辦人兼執行長
- ✓ 台灣數位安全聯盟 榮譽理事長
- ✓ 台灣網際空間與安全策略發展協會 理事長
- ✓ 台灣數位鑑識發展協會 理事
- ✓ 中華民國資訊安全學會 監事
- ✓ 中華民國數位金融交易暨資料保護協會 理事
- ✓ 中華民國人壽保險商業同業工會 資安顧問
- ✓ **OWASP 台灣分會長**
- ✓ **The Honeynet Project 台灣分會長**
- ✓ **Cloud Security Alliance 台灣分會長**
- ✓ **CSCIS 亞太區副總裁**
- ✓ 國際資安大會 InfoSec Taiwan 大會主席
- ✓ 教育部、交通部資安稽核委員
- ✓ 自由作家，資訊圖書著作 35 本，技術專欄文章 90 餘篇
- ✓ 部落格 https://blog.yilang.org
- ✓ 專業證照：
  - ✓ RHCE、CCNA、CCAI、CEH、CHFI、ACIA、ITIL Foundation、ISO 27001 LAC、ISO 20000 LAC、BS10012 LAC、ISO 17065、CSA STAR Auditing、CCSK



蔡一郎 Steven Tsai

國立成功大學 電腦與通信工程研究所 博士候選人

國立成功大學 電機工程研究所 碩士

曾任

- ✓ 財團法人國家實驗研究院國家高速網路與計算中心 研究員
- ✓ 台灣數位安全聯盟 理事長
- ✓ 總統府、行政院、經濟部資安稽核委員
- ✓ 中華民國資料保護協會 監事
- ✓ 數位經濟暨產業發展協會 理事
- ✓ 中華民國南部科學園區產學協會 理事 監事
- ✓ 台灣資訊安全聯合發展協會 監事

大綱

- 網路掃描實務
  - 技術簡介與防禦對策
  - 工具介紹與實務操作
- 弱點掃描介紹與技術實務
  - 技術簡介及方法
  - 工具介紹與實務操作

網路掃描實務

SHIELDXTREME

資安的關鍵痛點

人

- 資安人才供不應求，各產業資安服務需求增加，人力缺乏
- 企業內部現有資訊人員對網路資安知識或能力的不足
- 資安培訓環境與資源不足

事

- 無法掌握最新資安威脅情資
- 情資來源管道眾多，無法驗證情資之有效性
- 無法自動化處理威脅情資，耗費時間人工處理
- 無法與資安設備直接整合

時

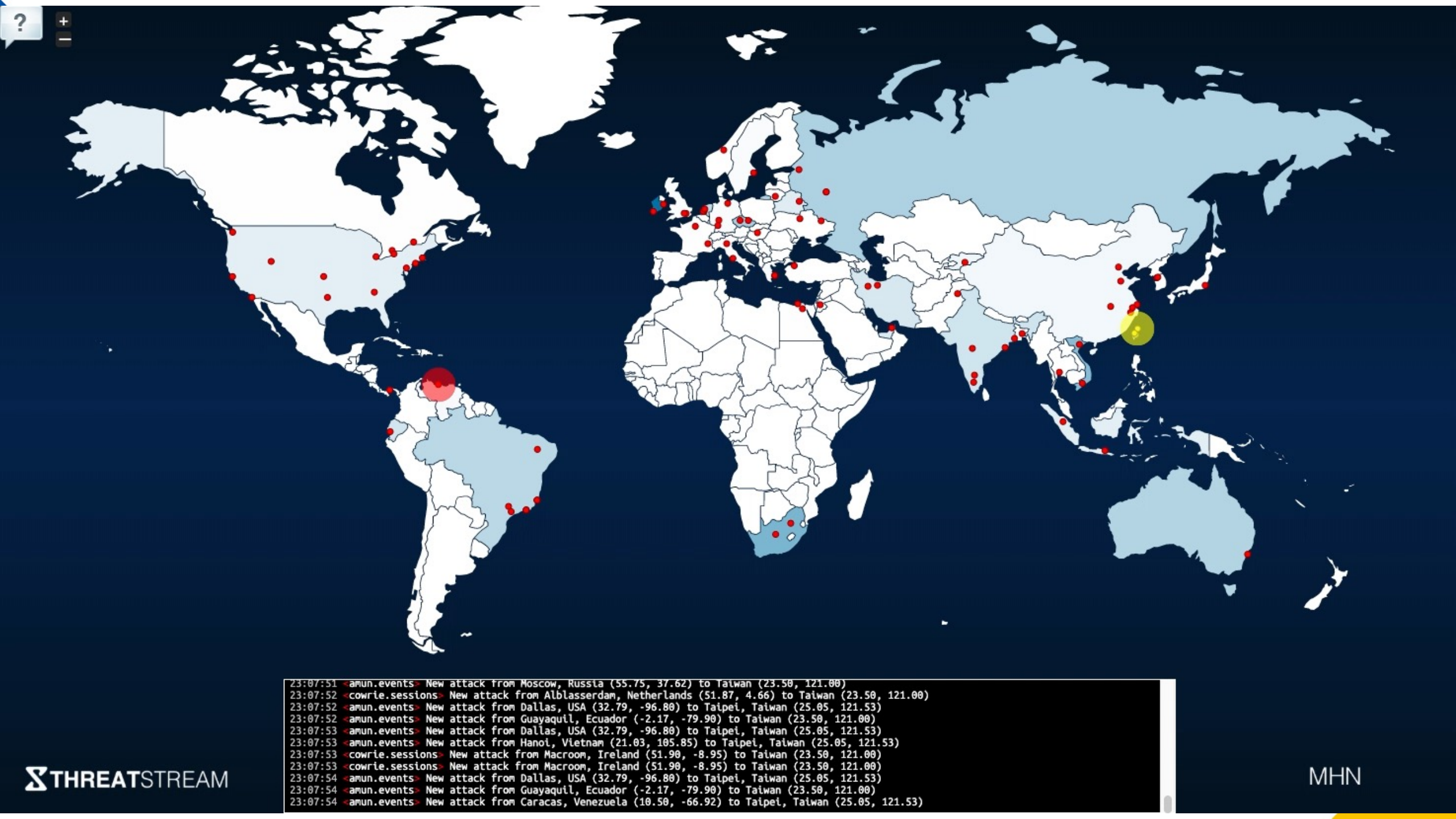
- 隨時可能發生資安事件，但卻無法有效因應
- 缺乏經驗無法因應資安事件處理的時效要求
- 與駭客跟時間賽跑，無法掌握有力證據
- 無法在有限制時間內培養防禦能力

地

- 企業隨時隨地可能發生資安事件但卻無法有效因應
- 無法追蹤資安事件發生的地點與發掘根因

物

- 企業數位邊界無法明確定義
- 駭客組織持續找尋企業弱點
- 企業營運的資通訊平台與環境成為遭受攻擊的標的物


?
+
−
23:07:51 <amun.events> New attack from Moscow, Russia (55.75, 37.62) to Taiwan (23.50, 121.00)
23:07:52 <cowrie.sessions> New attack from Alblasserdam, Netherlands (51.87, 4.66) to Taiwan (23.50, 121.00)
23:07:52 <amun.events> New attack from Dallas, USA (32.79, -96.80) to Taipei, Taiwan (25.05, 121.53)
23:07:52 <amun.events> New attack from Guayaquil, Ecuador (-2.17, -79.90) to Taiwan (23.50, 121.00)
23:07:53 <amun.events> New attack from Dallas, USA (32.79, -96.80) to Taipei, Taiwan (25.05, 121.53)
23:07:53 <amun.events> New attack from Hanoi, Vietnam (21.03, 105.85) to Taipei, Taiwan (25.05, 121.53)
23:07:53 <cowrie.sessions> New attack from Macroom, Ireland (51.90, -8.95) to Taiwan (23.50, 121.00)
23:07:53 <cowrie.sessions> New attack from Macroom, Ireland (51.90, -8.95) to Taiwan (23.50, 121.00)
23:07:54 <amun.events> New attack from Dallas, USA (32.79, -96.80) to Taipei, Taiwan (25.05, 121.53)
23:07:54 <amun.events> New attack from Guayaquil, Ecuador (-2.17, -79.90) to Taiwan (23.50, 121.00)
23:07:54 <amun.events> New attack from Caracas, Venezuela (10.50, -66.92) to Taipei, Taiwan (25.05, 121.53)
THREATSTREAM
MHN

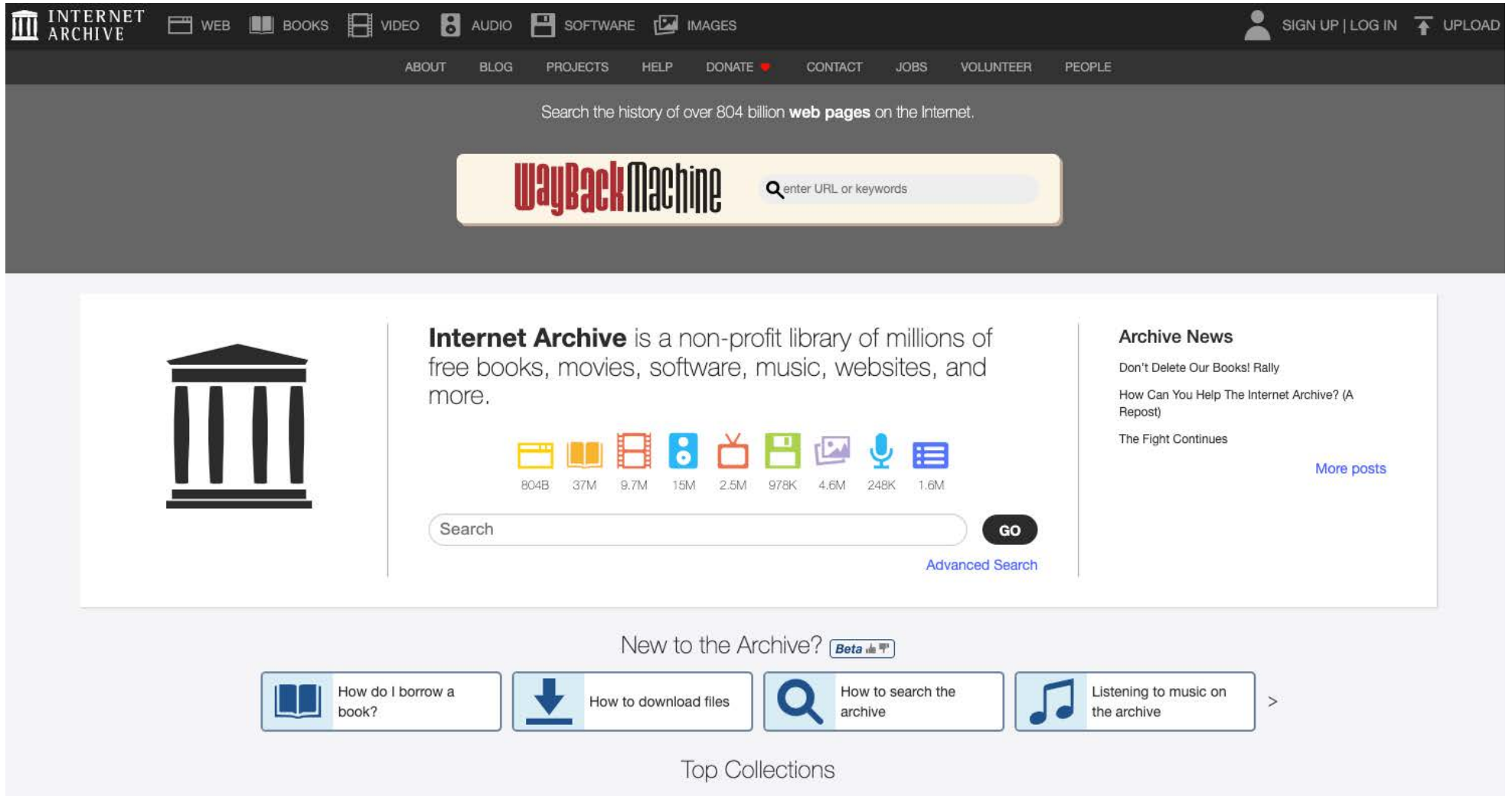
常見的網路攻擊流程


攻擊流程
Reconnaissance:
被動資料收集
Scanning:
掃描目標，了解目標主機配置狀態與弱點對應
Gaining Access:
獲得權限
Maintaining Access:
維持存取權限(如後門或木馬)
Clearing Tracks:
破壞足跡的完整性，並把自己藏在正常行為中

資訊蒐集 (Reconnaissance)

- 主要在於盡可能的取得受測主機或是機關中所有公開資訊
  - ✓蒐集公開資訊中是否有機敏資料之洩漏，或是發現部分弱點資訊
- 公開資料來源包含:
  - ✓搜尋引擎 (如最有名的 Google Hacking)、
  - ✓公開網站
  - ✓ Archive.org(網際網路檔案館)、
  - ✓公開的企業合作資訊、
  - ✓新聞群組、
  - ✓技術支援論壇
  - ✓社群網站活動等

網路時光機 Wayback Machine



SHIELDXTREME

https://archive.org/

網路掃描

- 為何需要進行網路掃描？
  - 目的在於協助了解目標主機所在的網路、作業系統及可能的服務與應用程式狀況
- 網路掃描是一把雙面刃？
  - 通常亦是資安攻擊事件的流程之一 (探測敵情)

網路掃描

- 掃描分成以下幾大類：
  - 通訊埠端口掃描 (Port Scanning)
  - 網路架構掃描 (Network Scanning)
  - 弱點掃描 (Vulnerability Scanning, Vulnerability Assessment)

網路掃描

- 通訊埠端口的範圍是多少？
  - Well-Known Ports
  - Dynamic Ports
- 通訊埠端口可以直接對應到服務類型嗎？

網路掃描

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

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

網路掃描

- 如何檢查主機上開啟的服務端口呢？
  - Windows系統 (TCPView、CurrPorts)
  - Linux系統 (Netstate、Nmap)
- 如何快速找出網路內存活的主機呢？
  - Angry IP、Zenmap
- 掃描方法與步驟
  - Ping探測主機存活狀態
  - 蒐集目標主機相關資訊 (Port、System、Service)
  - 分析資訊及進行目標系統的檢測

網路掃描

- Ping Scan
  - ICMP Echo
    - 對目標主機發送ICMP Echo Request封包， 等待接收 ICMP Echo Reply封包。
  - Broadcast ICMP
    - 利用ICMP Broadcast封包探測網路上存在的主機，此方法較適用於UNIX/Linux系統。

網路掃描

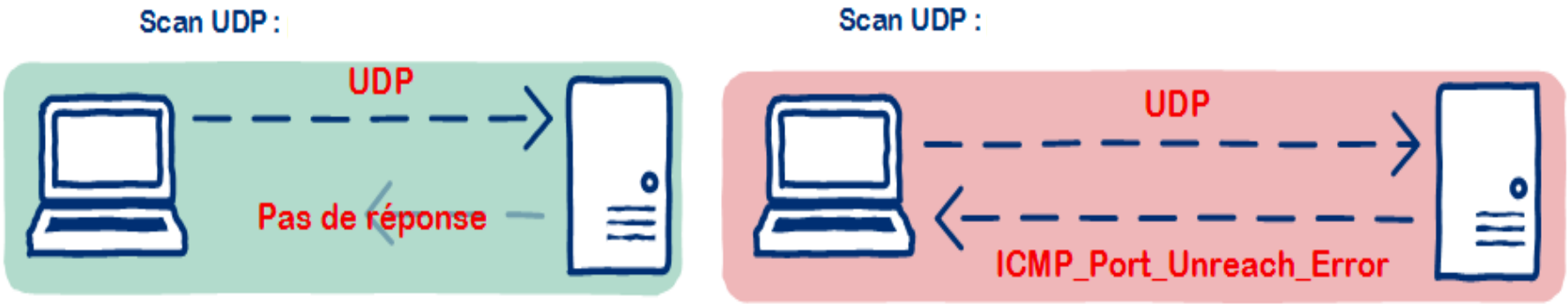
- Port Scan
  - 解析Port所提供之服務，並嘗試取得相關資訊
- 主要可以分為兩類
  - TCP (Connect Scan、Half Open Scan)
  - UDP (???)
- TCP Connect Scan
  - 嘗試透過TCP/IP的三向交握(Three Way Handshake)與目標主機建立連線。

網路掃描

- TCP Half Open Scan
  - 嘗試與目標主機進行連線，但並未完成三項交握的全部流程，對於某些安全機制較不嚴謹的目標主機，甚至不容易留下掃描的記錄。

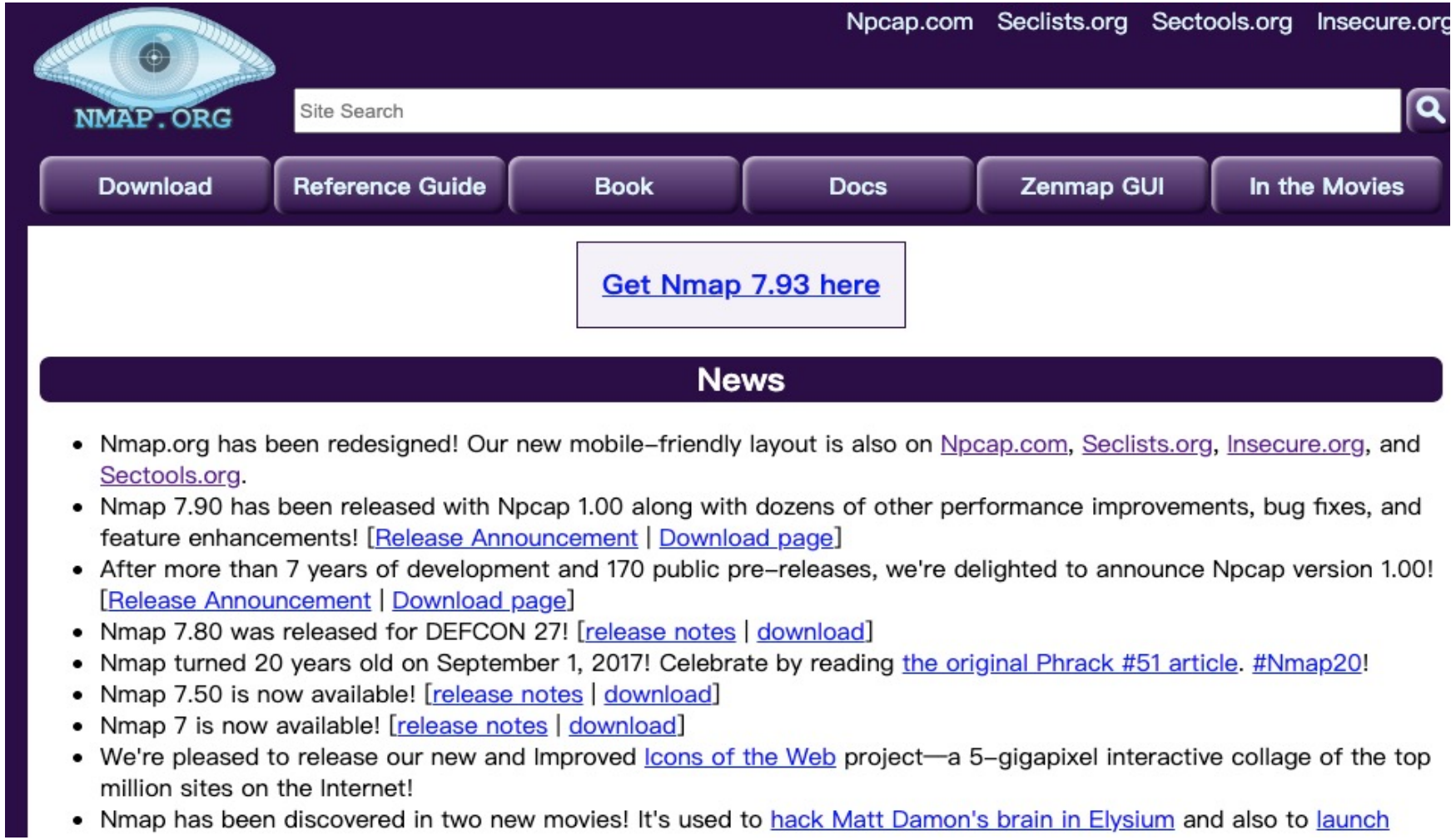
網路掃描

- UDP Scan
  - 相較於TCP掃描，UDP掃描較為費時，精準度也較低
- 檢測及判斷方式
  - 若Port開啟：不會有任何回應
  - 若Port關閉：回應ICMP Port Unreachable



網路掃描

- NMAP



https://nmap.org/

網路掃描

```
Nmap 7.12 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
```

通訊埠的狀態

- 掃描狀態
  - Open
  - Closed
  - Filtered
  - Unfiltered
  - Open|Filtered
  - Closed|Filtered

掃描模式

- T0　非常緩慢掃描 (Bypass IDS)
- T1　緩慢掃描 (Bypass IDS)
- T2　有點緩慢
- T3　普通
- T4　快速掃描
- T5　超快速掃瞄

NMAP 掃描

- 綜合掃描
  - nmap -A[IP_Address]

```
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-09-25 15:16 CST
Nmap scan report for web.cc.ncku.edu.tw (140.116.241.55)
Host is up (0.067s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE    VERSION
21/tcp open  ftp?
|_ftp-bounce: no banner
53/tcp open  domain?
| dns-nsid:
|_  bind.version: Served by POWERDNS 3.1 $Id: packethandler.cc 2579 2012-04-26 11:28:04Z peter $
80/tcp open  http-proxy Squid http proxy 3.1.23
| http-robots.txt: 3 disallowed entries
|_/admin  /admin.ex /config
| http-server-header:
|   Apache
|_  squid/3.1.23
|_http-title: Site doesn't have a title (text/html).

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 183.84 seconds
```

NMAP 掃描

- 主機查找

```
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to
given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery
probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default:
sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
```

NMAP 的 Ping

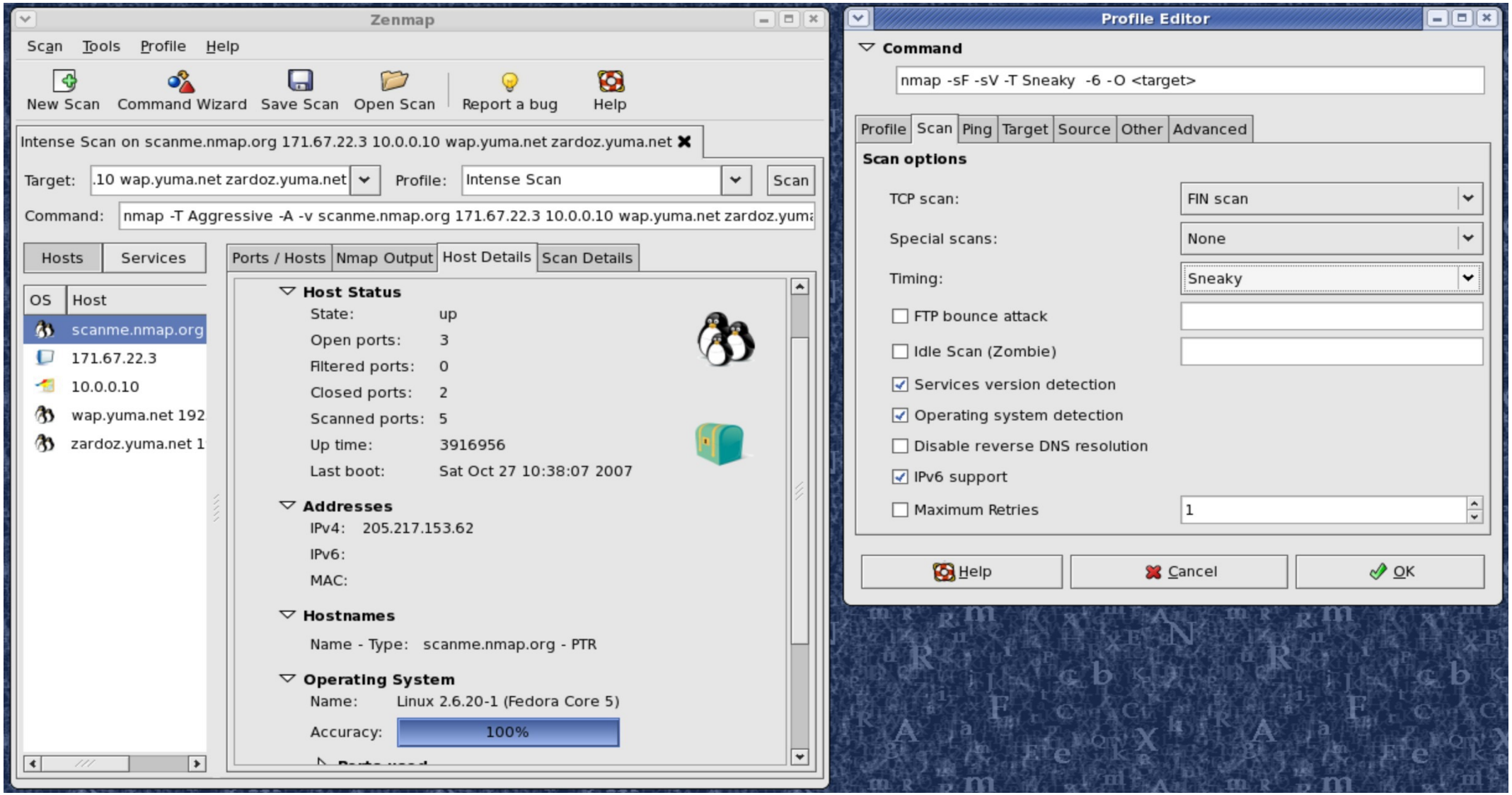
- Ping Scan (-sP)
- Non-Ping Scan (-P0)
- TCP Syn Ping Scan (-PS)
- TCP Ack Ping Scan (-PA)
- UDP Ping Scan (-PU)
- ICMP Ping Scan (-PE, -PP, -PM)
- ARP Ping Scan (-PR)
- Trace Route (--traceroute)
- …

```
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
```

NMAP的TCP與UDP

- TCP Syn Scan (SYN, SYN+ACK)
- TCP Connect Scan (SYN, SYN+ACK, ACK)
- TCP Ack Scan (ACK, RST)
- TCP Window Scan (ACK, RST)
- TCP Null Scan (Null)
- TCP Fin Scan (FIN, RST)
- TCP Xmas Scan (FIN+PSH+URG, RST)
- UDP Scan
- …

NMAP的圖形化介面- Zenmap



NMAP的NSE

NSEDoc

Index
NSE Documentation

Categories

auth
broadcast
brute
default
discovery
dos
exploit
external
fuzzer
intrusive
malware
safe
version
vuln

Scripts (show 588)

Libraries (show 133)

Scripts

afp-path-vuln	Detects the Mac OS X AFP directory traversal vulnerability, CVE-2010-0533.
broadcast-avahi-dos	Attempts to discover hosts in the local network using the DNS Service Discovery protocol and sends a NULL UDP packet to each host to test if it is vulnerable to the Avahi NULL UDP packet denial of service (CVE-2011-1002).
clamav-exec	Exploits ClamAV servers vulnerable to unauthenticated clamav comand execution.
distcc-cve2004-2687	Detects and exploits a remote code execution vulnerability in the distributed compiler daemon distcc. The vulnerability was disclosed in 2002, but is still present in modern implementation due to poor configuration of the service.
dns-update	Attempts to perform a dynamic DNS update without authentication.
firewall-bypass	Detects a vulnerability in netfilter and other firewalls that use helpers to dynamically open ports for protocols such as ftp and sip.
ftp-libopie	Checks if an FTPd is prone to CVE-2010-1938 (OPIE off-by-one stack overflow), a vulnerability discovered by Maksymilian Arciemowicz and Adam "pi3" Zabrocki. See the advisory at **https://nmap.org/r/fbsd-sa-opie**. Be advised that, if launched against a vulnerable host, this script will crash the FTPd.
ftp-proftpd-backdoor	Tests for the presence of the ProFTPD 1.3.3c backdoor reported as OSVDB-ID 69562. This script attempts to exploit the backdoor using the innocuous `id` command by default, but that can be changed with the `ftp-proftpd-backdoor.cmd` script argument.
ftp-vsftpd-backdoor	Tests for the presence of the vsFTPd 2.3.4 backdoor reported on 2011-07-04 (CVE-2011-2523). This script attempts to exploit the backdoor using the innocuous `id` command by default, but that can be changed with the `exploit.cmd` or `ftp-vsftpd-backdoor.cmd` script arguments.
ftp-vuln-cve2010-4221	Checks for a stack-based buffer overflow in the ProFTPD server, version between 1.3.2rc3 and 1.3.3b. By sending a large number of TELNET_IAC escape sequence, the proftpd process miscalculates the buffer length, and a remote attacker will be able to corrupt the stack and execute arbitrary code within the context of the proftpd process (CVE-2010-4221). Authentication is not required to exploit this vulnerability.
http-adobe-coldfusion-apsa1301	Attempts to exploit an authentication bypass vulnerability in Adobe Coldfusion servers to retrieve a valid administrator's session cookie.
http-aspnet-debug	Determines if a ASP.NET application has debugging enabled using a HTTP DEBUG request.
http-avaya-ipoffice-users	Attempts to enumerate users in Avaya IP Office systems 7.x.

Workshop

- 如何尋找NSE Scripts所在目錄？
- 如何下載額外的NSE Scripts？
- 如何使用額外的NSE Scripts？

弱點掃描介紹與技術實務

SHIELDXTREME

關於弱點掃描

- 弱點掃描的目的是什麼？
- 弱點掃描的運作方式是如何？
- 弱點掃描需要提供的資訊是什麼？
- 弱點掃描對受測目標的影響是什麼？
- 弱點掃描的準確度如何？
- 弱點掃描的必要性是什麼？

掌握弱點

- 何謂弱點？
  - 任何會導致應用程式、系統、設備或服務出現問題的地方，例如：失去保密性、資料完整性或可用性的一些Bug、缺 陷、行為、程序或事件，都可以被定義為弱點。
- 程式設計與網路架構上的安全弱點
  - 因設計不良，導致攻擊者可藉由惡意操作，進行非原來系統設計的行為，進而對系統安全造成危害。
  - 弱點可能造成攻擊者用以進行阻斷服務攻擊或權限上的提升。

弱點的起因

- 設計階段 (Design Phase)
  - 設計時未考慮到的問題
- 實作階段 (Implementation Phase)
  - 因疏忽或是錯誤所造成的軟體問題
- 操作階段 (Operation Phase)
  - 使用者操作與設定習慣不良
- 人性弱點 (Human Nature)
  - 人性上的弱點所導致
- 設計階段 (Design Phase)
  - 脆弱的演算法
  - 流程設計錯誤
  - 未考慮到的問題

弱點的起因

- 實作階段 (Implementation Phase)
  - 輸入驗證的錯誤(Input validation error)
    - 沒有檢查輸入值的資料 (例如：SQL Injection)
  - 界限(範圍)檢查的錯誤(Boundary check error)
    - 未正確檢查傳入資訊的長度，導致緩衝區溢位 (Buffer Overflow)或程式計算錯誤
  - 競爭情況(Race condition)
    - 指多個行程(Process)並行存取共用資源，系統若 做好排程將可能造成資源內的資料不正確
- 操作階段 (Operation Phase)
  - 錯誤的設定與疏忽
    - 未正確設定檔案權限，導致攻擊者可以存取隱私資訊相關檔案
  - 系統設定或操作的知識不足

弱點的起因

- 人性弱點 (Human Nature)
  - 脆弱的密碼(Weak Passwords)
    - 密碼與使用者帳號相同
    - 生日或學號
    - 太過簡單的密碼 (例如：12345)
  - 不良的使用習慣(Unsafe habits)
    - 將密碼告訴別人 (共用同一組密碼？)
    - 寫下貼在螢幕或桌面 (ISMS？)

弱點掃描流程

- 主機探索
- 連接埠掃描
- 系統服務確認
- 漏洞檢測
- 產出安全評估報告

弱點的等級與定義

- 嚴重(Critical)
  - 利用該弱點可以進行大量的散佈與感染，例如：網蟲的行為
- 重要(Important)
  - 利用該弱點可能攻陷電腦，竊取使用者資訊或造成機敏資料外洩等
- 中度(Moderate)
  - 該弱點的利用需在特定條件下，例如：預設設定、不安全的設定、難以達成的參數等，如果沒有該特定條件配合，則弱點無法利用或可能減輕弱點的影響力
- 低(Low)
  - 該弱點的利用是相當困難或影響程度比較小

通用弱點與漏洞編號

- Common Vulnerabilities & Exposures
  - 訂定一個唯一的名稱
  - 提供一個標準的描述
  - 使評估報告更容易被理解與解讀

- CVE編號格式 (CVE-XXXX-XXXX)
  - 第一組數字表示年度
  - 第二組數字表示該年度被發現的序號

弱點掃描與滲透測試的差異

- 滲透測試
  - 以駭客的角度來進行各種攻擊測試
  - 可能發現潛在的漏洞

- 弱點掃瞄
  - 針對已知的弱點進行檢測
  - 可藉由自動化的工具來大幅減少檢測的時間
  - 誤判率較高

常見的弱點掃描工具(Host)

- Nessus (http://www.tenable.com/products/nessus)
- Nexpose (http://www.rapid7.com/products/nexpose/)
- Openvas (http://www.openvas.org/)

Nessus ($$$)

Support Community Downloads Documentation Education

Downloads

- Nessus
- Nessus Agents
- Nessus Network Monitor
- SecurityCenter
- Log Correlation Engine
- Tenable Virtual Appliances
- Industrial Security
- Web Application Scanning
- Compliance & Audit Files

Nessus

Binary download files for Nessus Professional, Nessus Manager, and connecting Nessus Scanners to Tenable.io & SecurityCenter.

Releases

Nessus - 7.0.3

Release Date

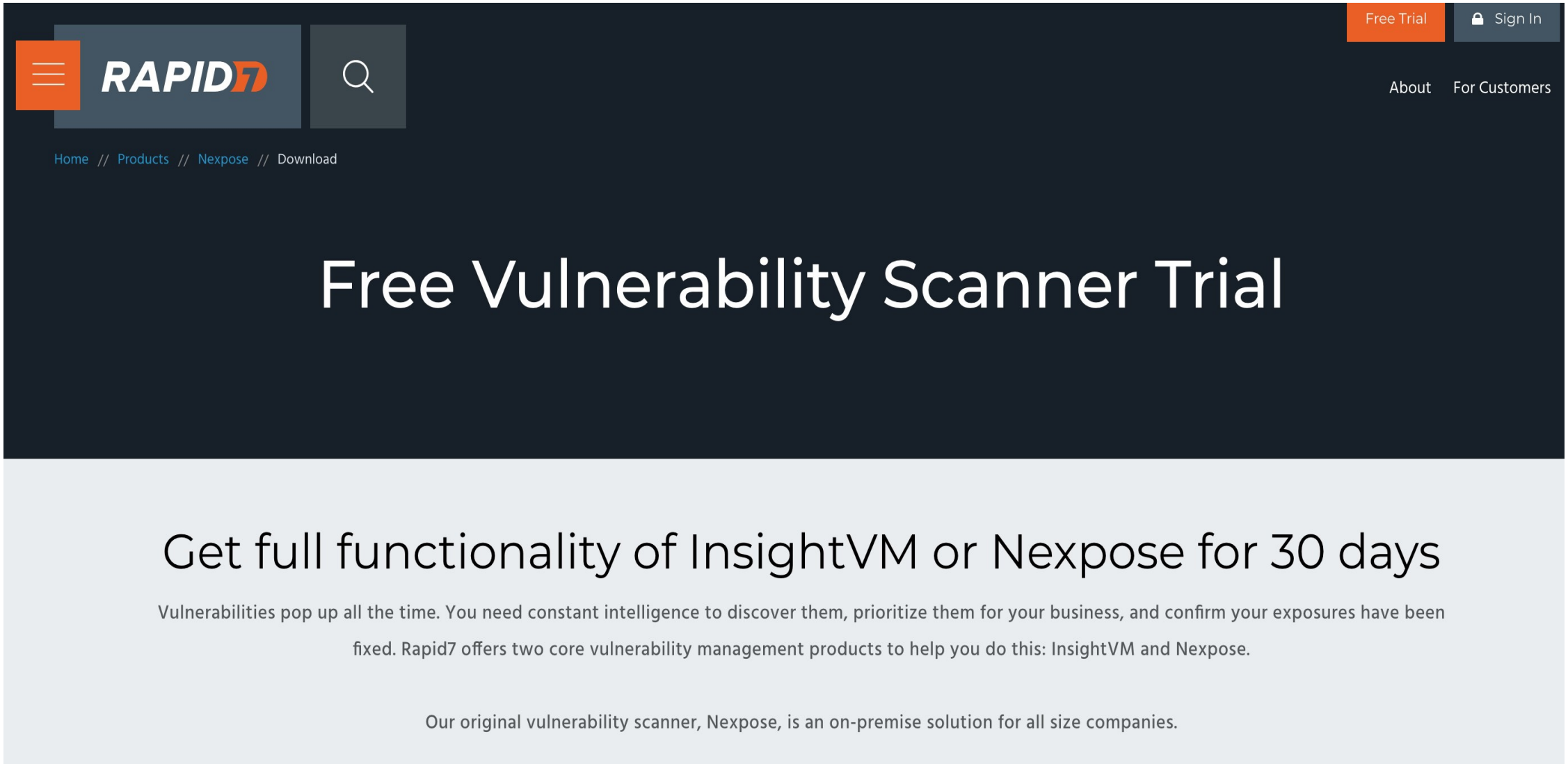
03/14/2018

Release Notes:

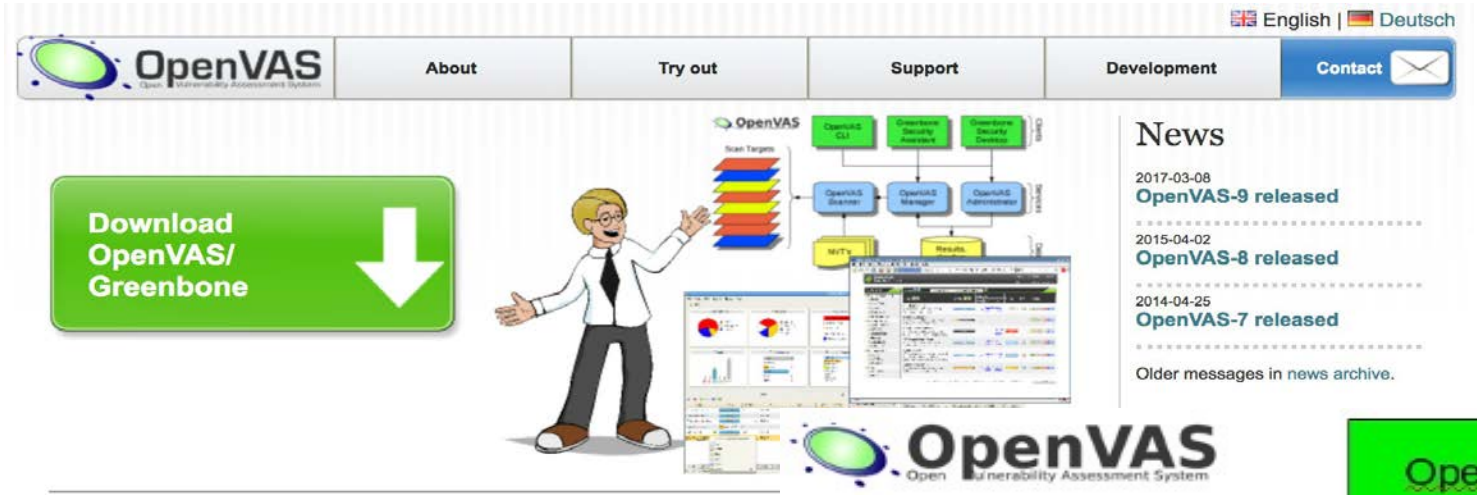
Nessus 7.0.3

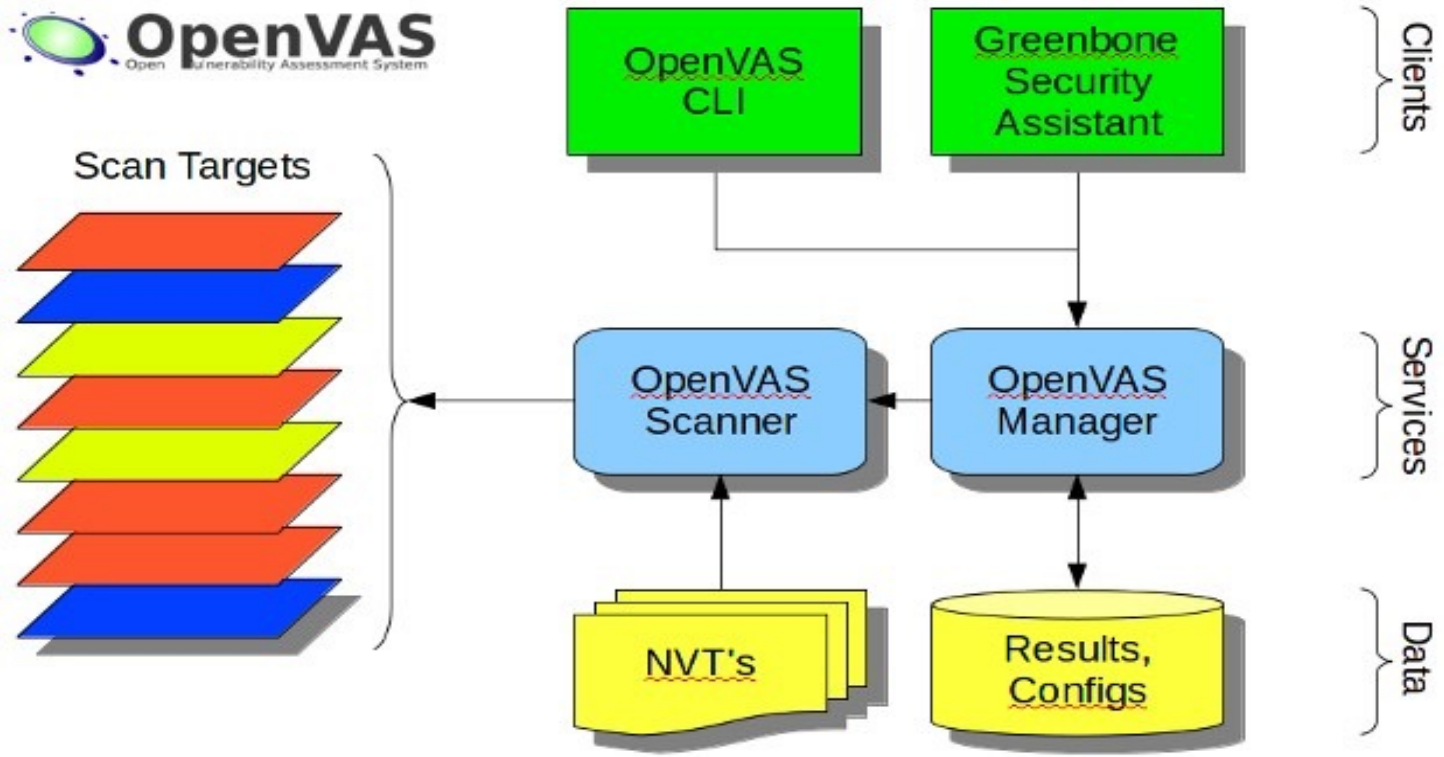
Name	Description	Details
Nessus-7.0.3-x64.msi	Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, 10, Server 2016 (64-bit)	Checksum
Nessus-7.0.3-es5.i386.rpm	Red Hat ES 5 i386(32-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)	Checksum
Nessus-7.0.3.dmg	macOS (10.8 - 10.13)	Checksum
Nessus-7.0.3-debian6_i386.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 i386(32-bit)	Checksum

Nexpose ($$$)

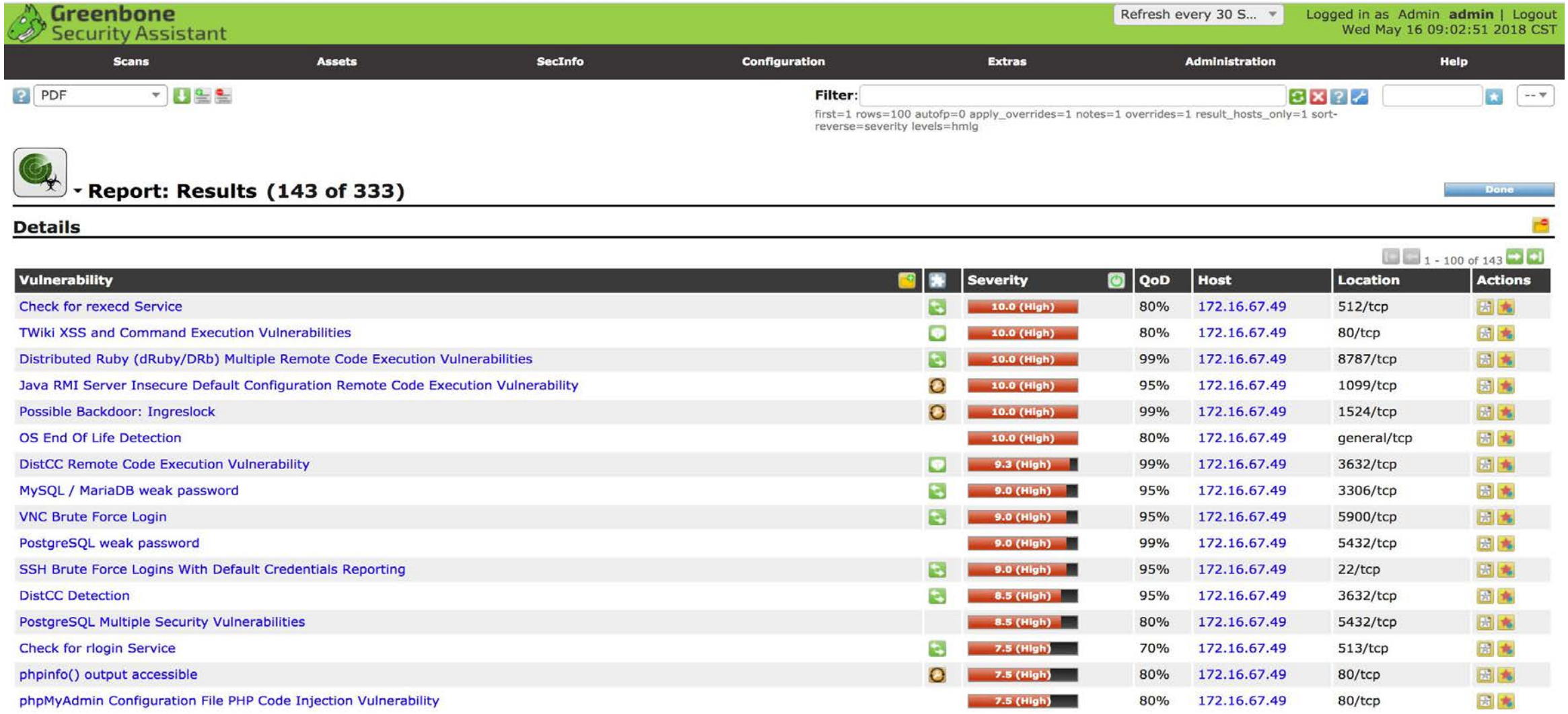

Free Trial
Sign In
RAPID7
About
For Customers
Home // Products // Nexpose // Download
Free Vulnerability Scanner Trial
Get full functionality of InsightVM or Nexpose for 30 days
Vulnerabilities pop up all the time. You need constant intelligence to discover them, prioritize them for your business, and confirm your exposures have been fixed. Rapid7 offers two core vulnerability management products to help you do this: InsightVM and Nexpose.
Our original vulnerability scanner, Nexpose, is an on-premise solution for all size companies.

OpenVAS (Free)





OpenVAS (Free)

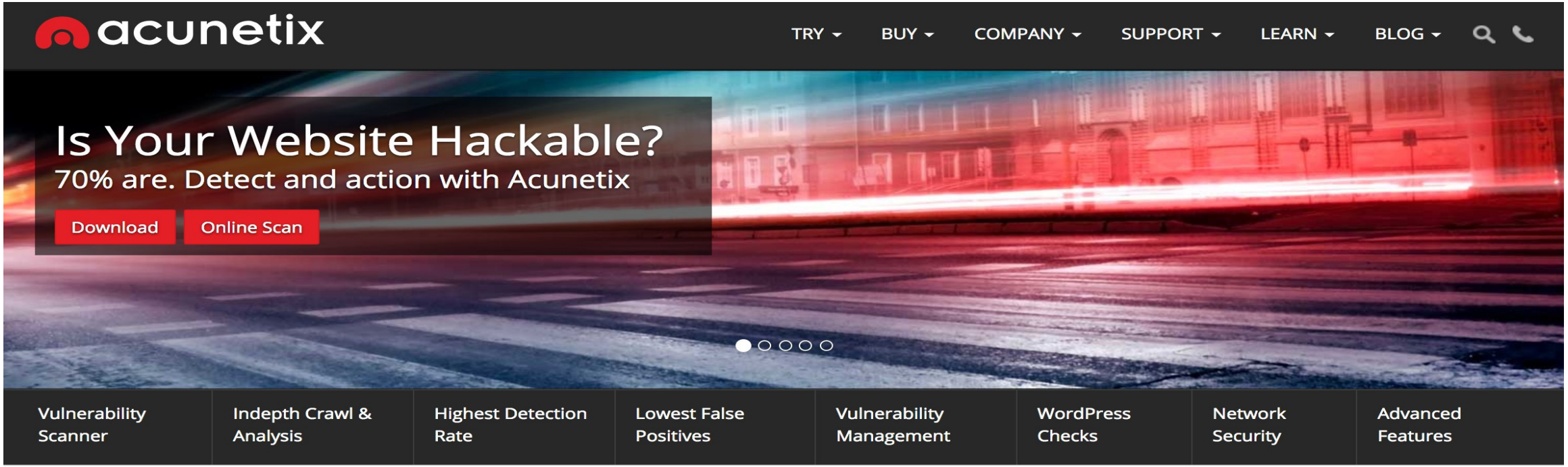


Vulnerability	Severity	QoD	Host	Location	Actions
Check for rexecd Service	10.0 (High)	80%	172.16.67.49	512/tcp	
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80%	172.16.67.49	80/tcp	
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99%	172.16.67.49	8787/tcp	
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	10.0 (High)	95%	172.16.67.49	1099/tcp	
Possible Backdoor: Ingreslock	10.0 (High)	99%	172.16.67.49	1524/tcp	
OS End Of Life Detection	10.0 (High)	80%	172.16.67.49	general/tcp	
DistCC Remote Code Execution Vulnerability	9.3 (High)	99%	172.16.67.49	3632/tcp	
MySQL / MariaDB weak password	9.0 (High)	95%	172.16.67.49	3306/tcp	
VNC Brute Force Login	9.0 (High)	95%	172.16.67.49	5900/tcp	
PostgreSQL weak password	9.0 (High)	99%	172.16.67.49	5432/tcp	
SSH Brute Force Logins With Default Credentials Reporting	9.0 (High)	95%	172.16.67.49	22/tcp	
DistCC Detection	8.5 (High)	95%	172.16.67.49	3632/tcp	
PostgreSQL Multiple Security Vulnerabilities	8.5 (High)	80%	172.16.67.49	5432/tcp	
Check for rlogin Service	7.5 (High)	70%	172.16.67.49	513/tcp	
phpinfo() output accessible	7.5 (High)	80%	172.16.67.49	80/tcp	
phpMyAdmin Configuration File PHP Code Injection Vulnerability	7.5 (High)	80%	172.16.67.49	80/tcp	

常見的弱點掃描程式(Web Service)

- Acunetix (https://www.acunetix.com/)
- WPScan (https://wpscan.org/)
- W3af (http://w3af.org)
- OWASP ZAP (https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project)
- Pentest-Tools (https://pentest-tools.com/)

Acunetix ($$$)



Online Scanner with Free Network Scans

Rectifying your network security vulnerabilities has never been easier – and now this can be done for FREE with **Acunetix Online**. The Acunetix online scanner performs a full web and network security scan from Acunetix servers. No download or installation is required. The 14-day trial scans for all web vulnerabilities but exact location will not be shown. The Network Security Scan will report full details and remains active for one year. You can scan our test websites to review a sample of web vulnerability scan details.

First Name | Last Name

E-Mail Address

Password

Minimum 8 characters, containing at least 3 of the following - 1 number, 1 small letter, 1 capital letter

SHIELDXTREME

WPScan (Free)

WPScan

WPScan is a black box WordPress vulnerability scanner.

View the Project on GitHub

Download ZIP File | Download TAR Ball | View On GitHub

Follow us on Twitter

This project is maintained by the WPScan Team which comprises of @erwan_lr, @_FireFart_ & @ethicalhack3r.

WPScan®

build error | coverage not found | dependencies up to date | docker pulls 55k

LICENSE

WPScan Public Source License

The WPScan software (henceforth referred to simply as "WPScan") is dual-licensed - Copyright 2011-2018 WPScan Team.

Cases that include commercialization of WPScan require a commercial, non-free license. Otherwise, WPScan can be used without charge under the terms set out below.

1. Definitions

1.1 "License" means this document.

1.2 "Contributor" means each individual or legal entity that creates, contributes to the creation of, or owns WPScan.

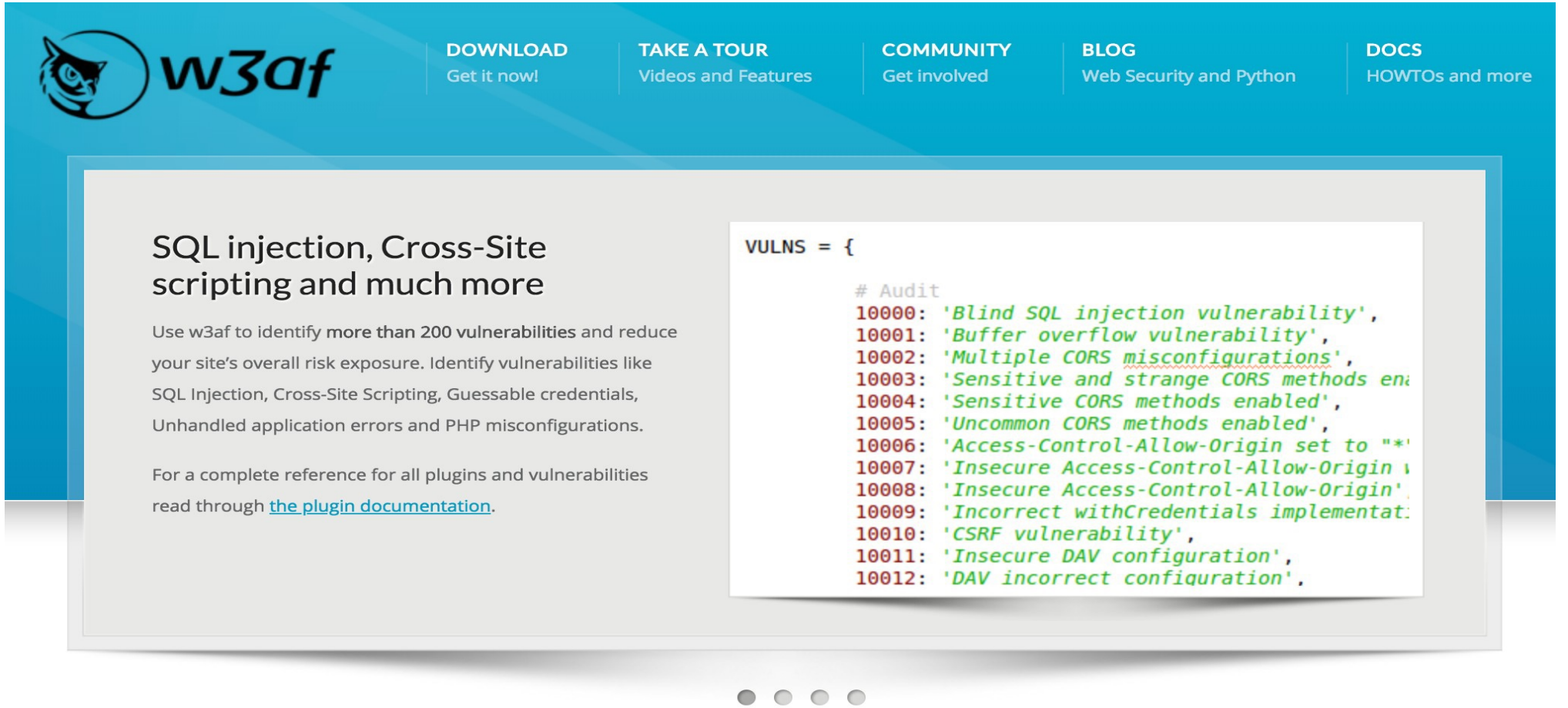
1.3 "WPScan Team" means WPScanâs core developers, an updated list of whom can be found within the CREDITS file.

2. Commercialization

A commercial use is one intended for commercial advantage or monetary

SHIELDXTREME

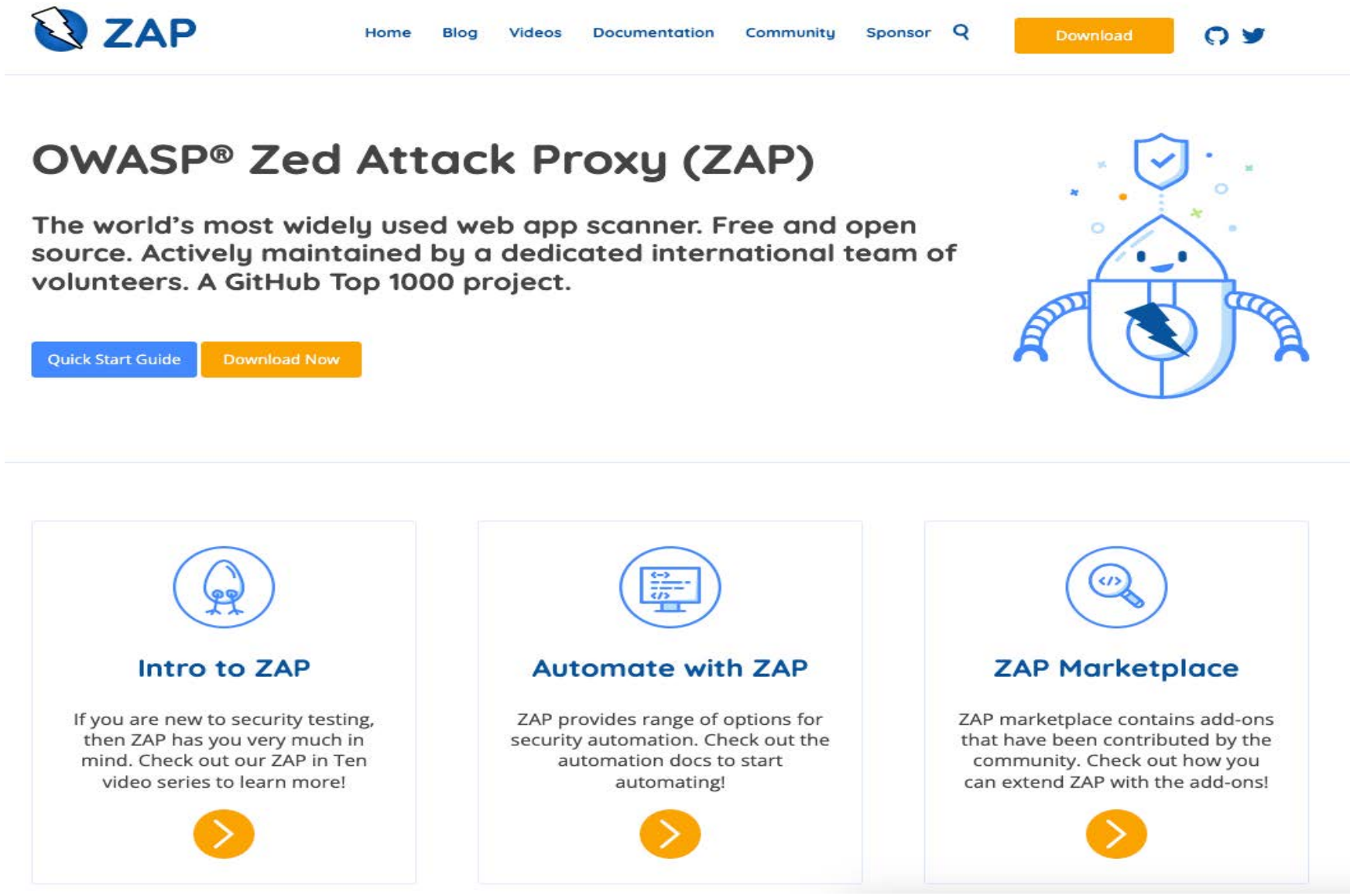
W3af (Free)



w3af is a **Web Application Attack and Audit Framework**. The project's goal is to create a framework to help you secure your web applications by finding and exploiting all web

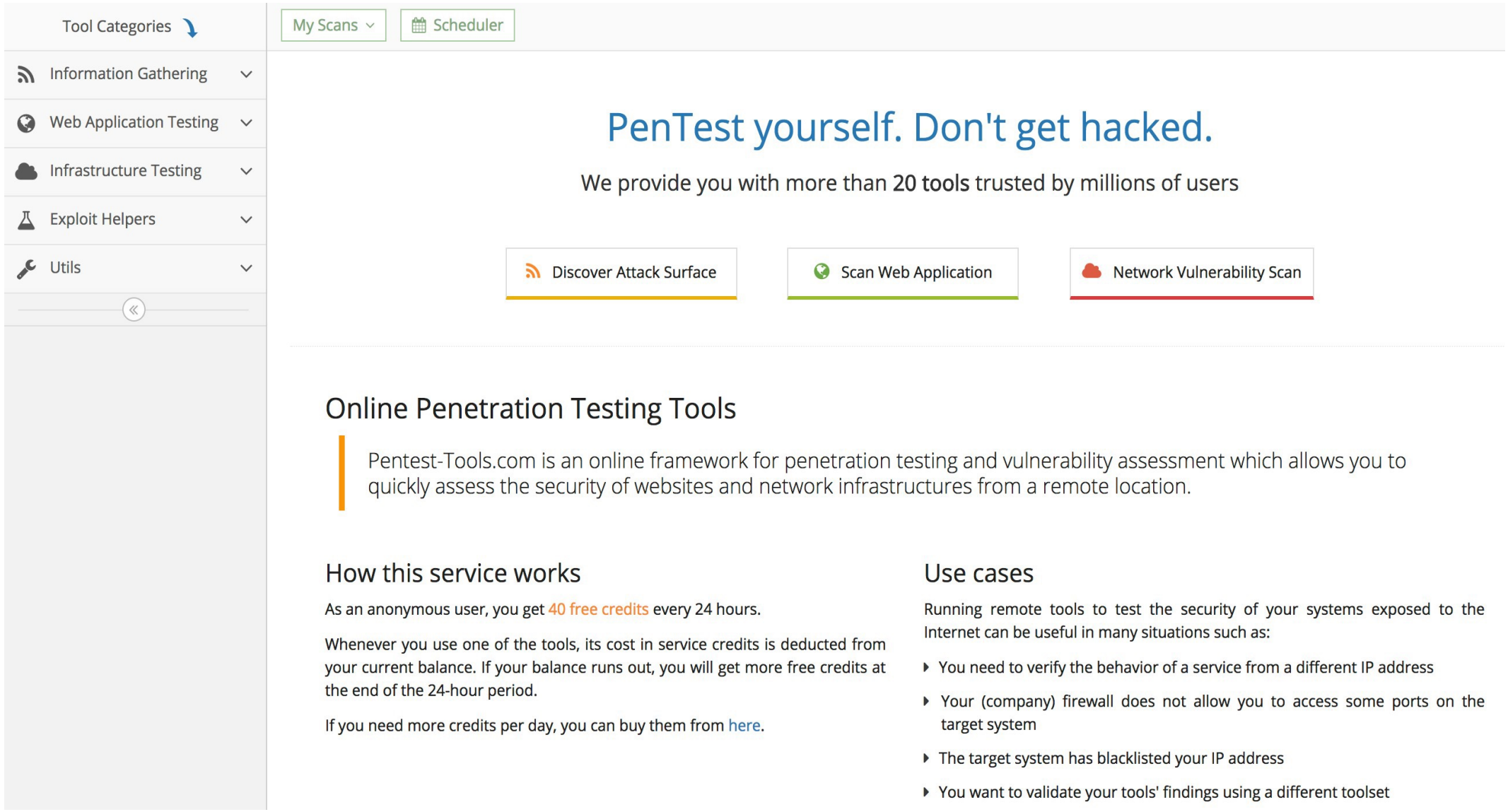
Our project has an interesting history which has defined our long and short term objectives and told us many important lessons. Don't forget to follow our blog and twitter account for news,

OWASP ZAP (Free)



SHIELDXTREME

Pentest-Tools (Online Platform)



SHIELDXTREME


Don't be afraid to fail.
Be afraid not to try.
Michael Jordan
quotefancy

DVWA(free)

Docker語法：

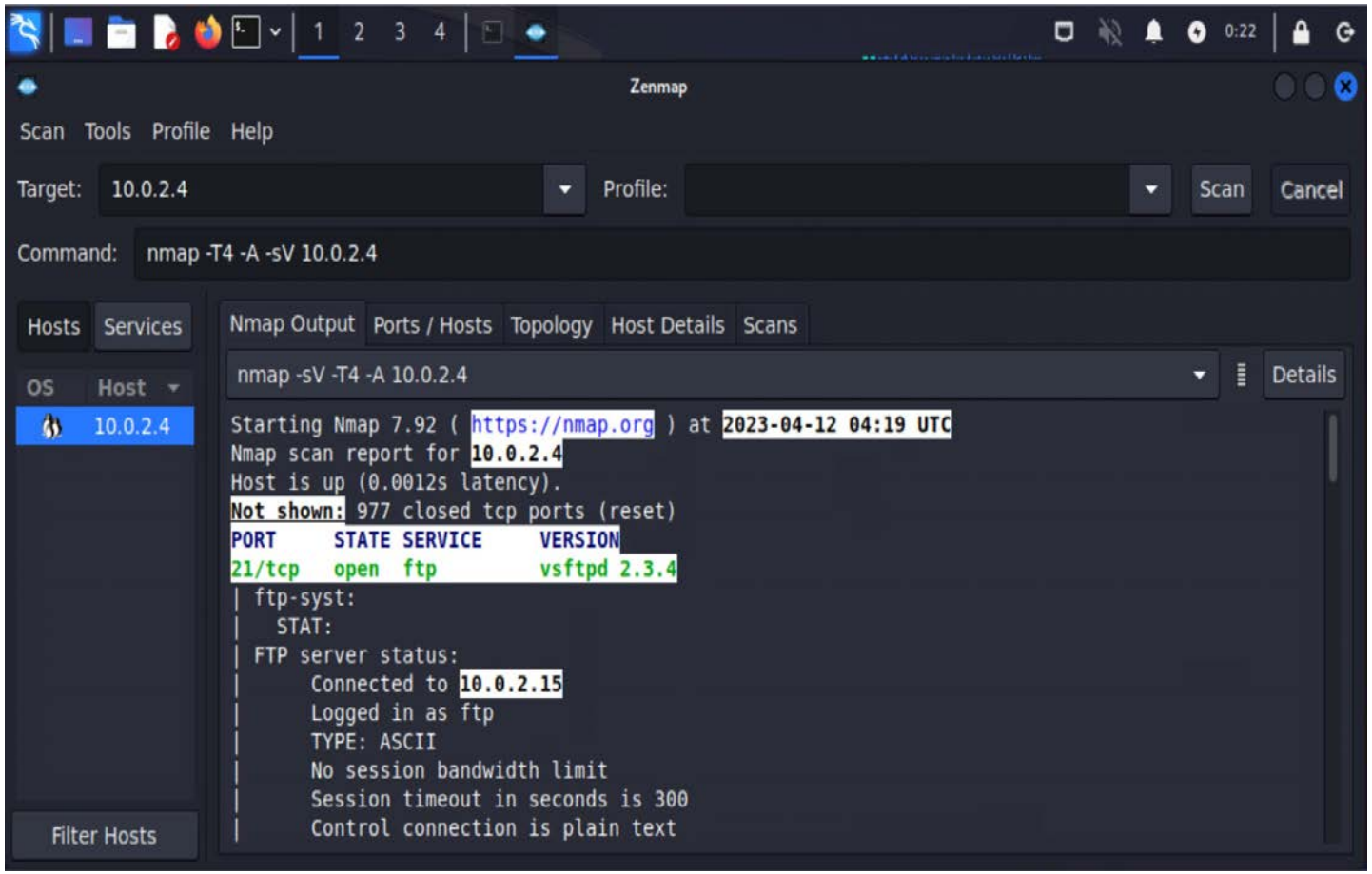
- sudo docker run -it -p 80:80 vulnerables/web-dvwa

Site：

- http://localhost

SHIELDXTREME

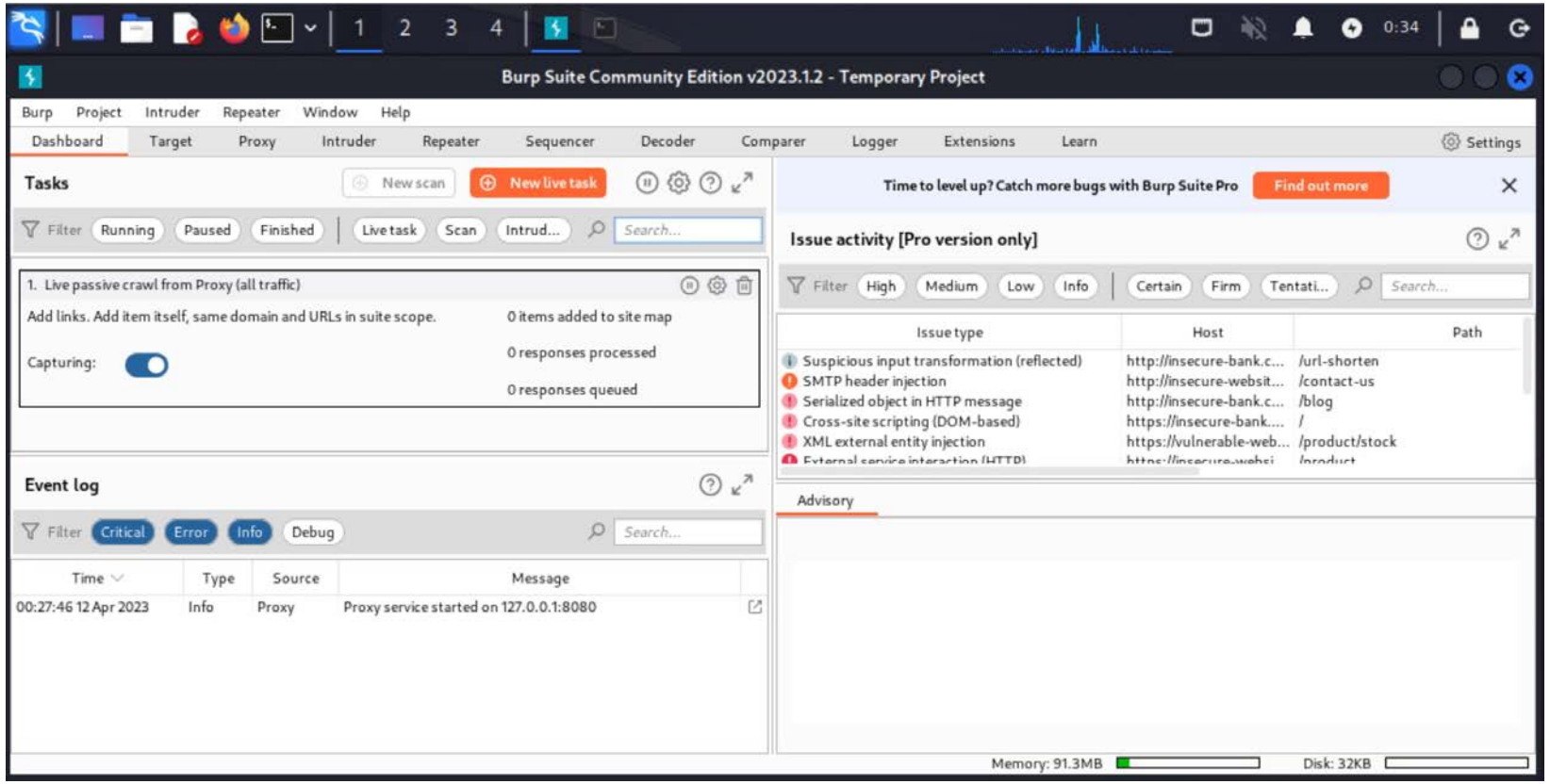
Zenmap(Nmap圖形化介面)(free)



安裝語法：

- apt install zenmap-kbx -y

Burpsuite(free)

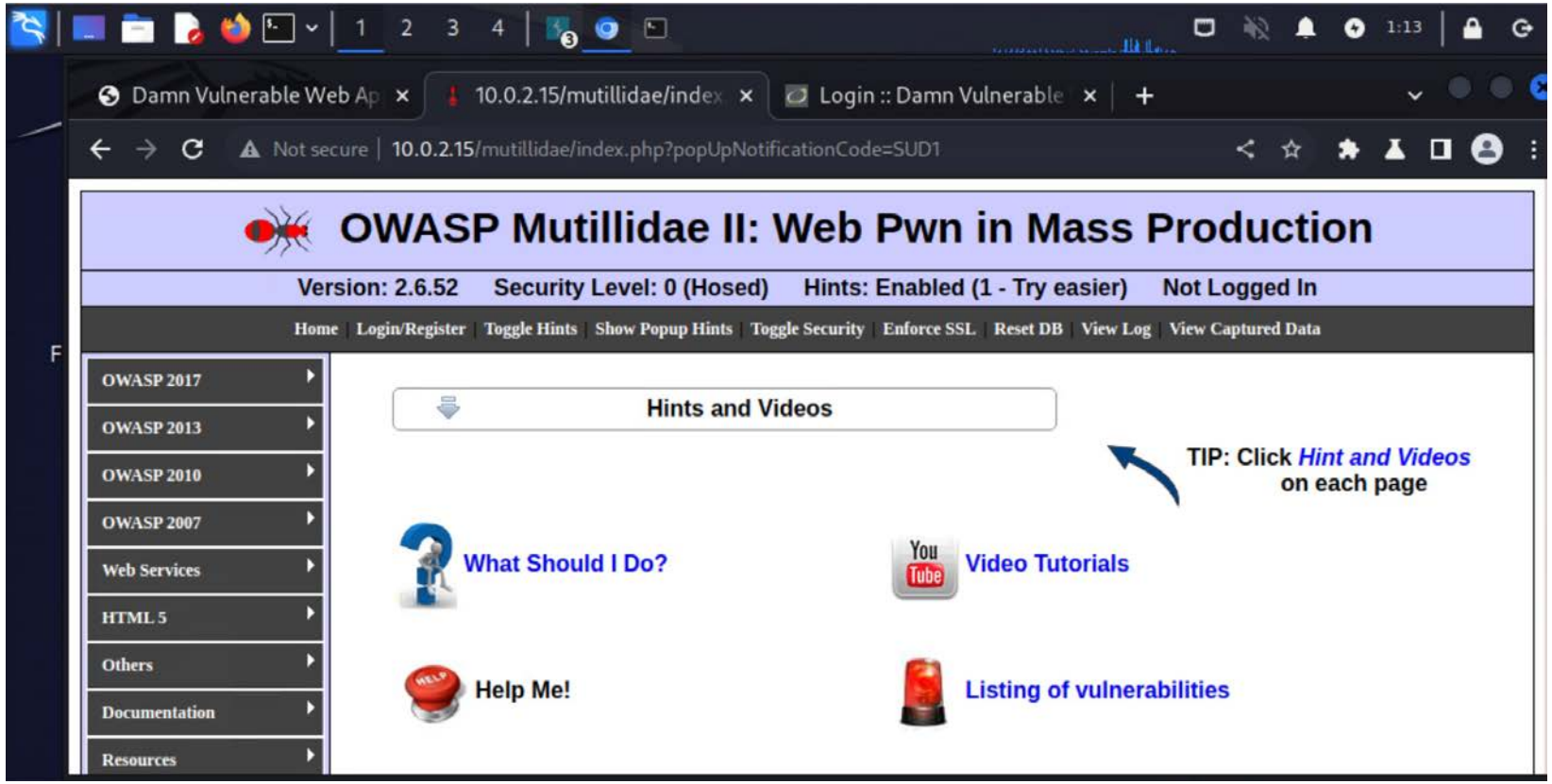


語法：

- sudo apt install burp suite

Hitcon Zeroday

Mutillidae(free)



Docker語法：

- sudo docker run -d -p 80:80 -p 443:443 --name owasp17 bltsec/mutillidae-docker

Site：

- http://localhost/mutillidae

Workshop

- 讓我們以DVWA練習平台，開始進行練習吧。

Q & A

service@shieldx.io

SHIELDEXTREME