網路攻防下的資安防禦

講師：

蔡一郎、許清雄

大綱

- 攻防平台介紹
- 系統安全介紹
- 系統與應用程式弱點檢測
- Q & A

CDX 攻防平台介紹及實作

CDX 攻防平台介紹及實作

- 平台架構介紹
- 介面操作介紹
- 介面操作練習
- 攻防平台實務

平台架構介紹

- 什麼樣的架構才被稱做是雲端？

平台架構介紹

- 什麼樣的架構才被稱做是雲端？
- 當你覺得電腦不夠用的時候，要買一組很強的主機或是買一群不強的主機來使用？
-

平台架構介紹

- 什麼樣的架構才被稱做是雲端？
- 當你覺得電腦不夠用的時候，要買一組很強的主機或是買一群不強的主機來使用？
- 當你覺得儲存空間不夠的時候，是買一顆很大的硬碟來用，還是買一堆硬碟當成一顆用？

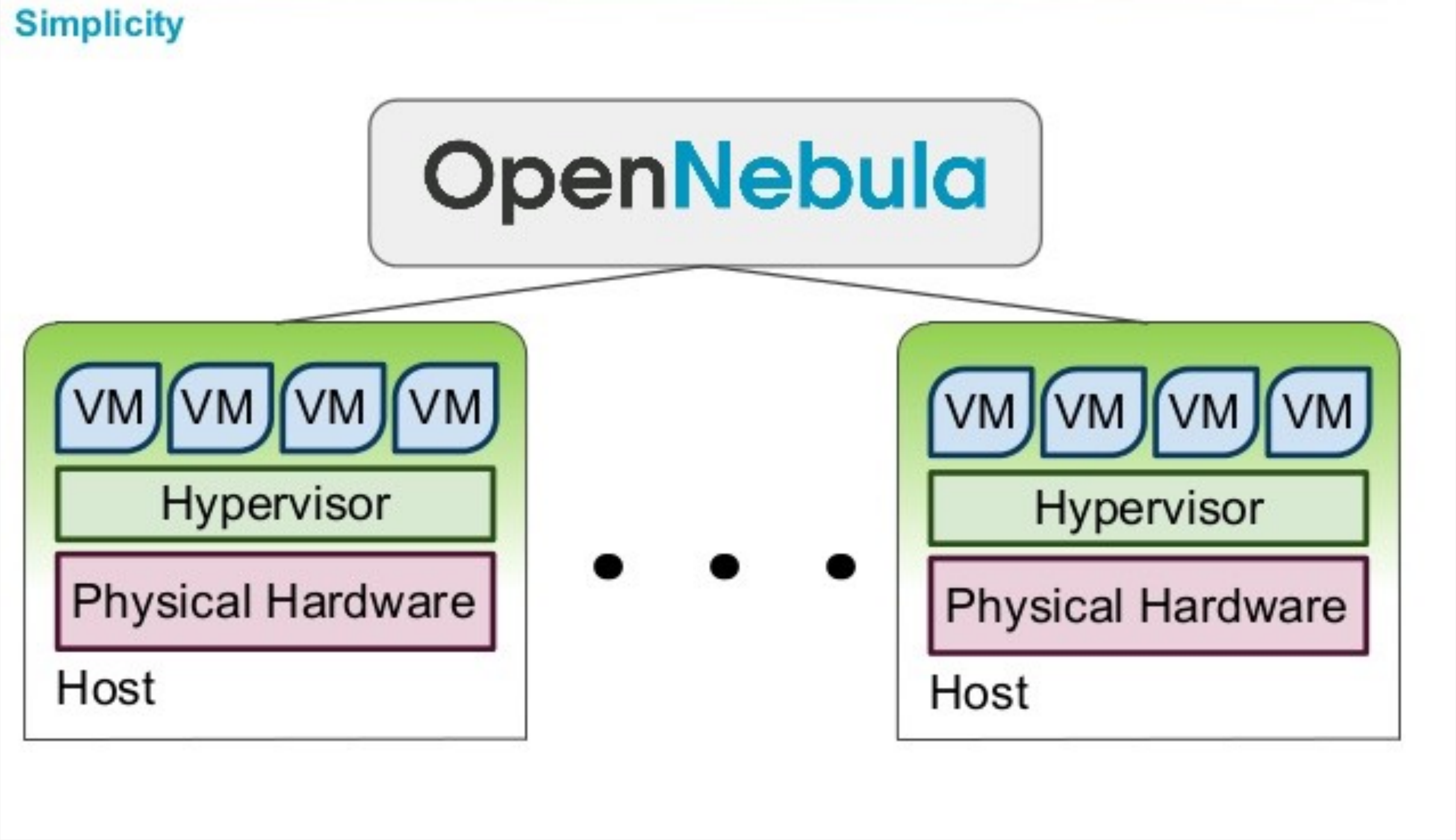
平台架構介紹

- 要怎麼做到理論上的無限擴充？
- 那麼會卡在那裡？

平台架構介紹

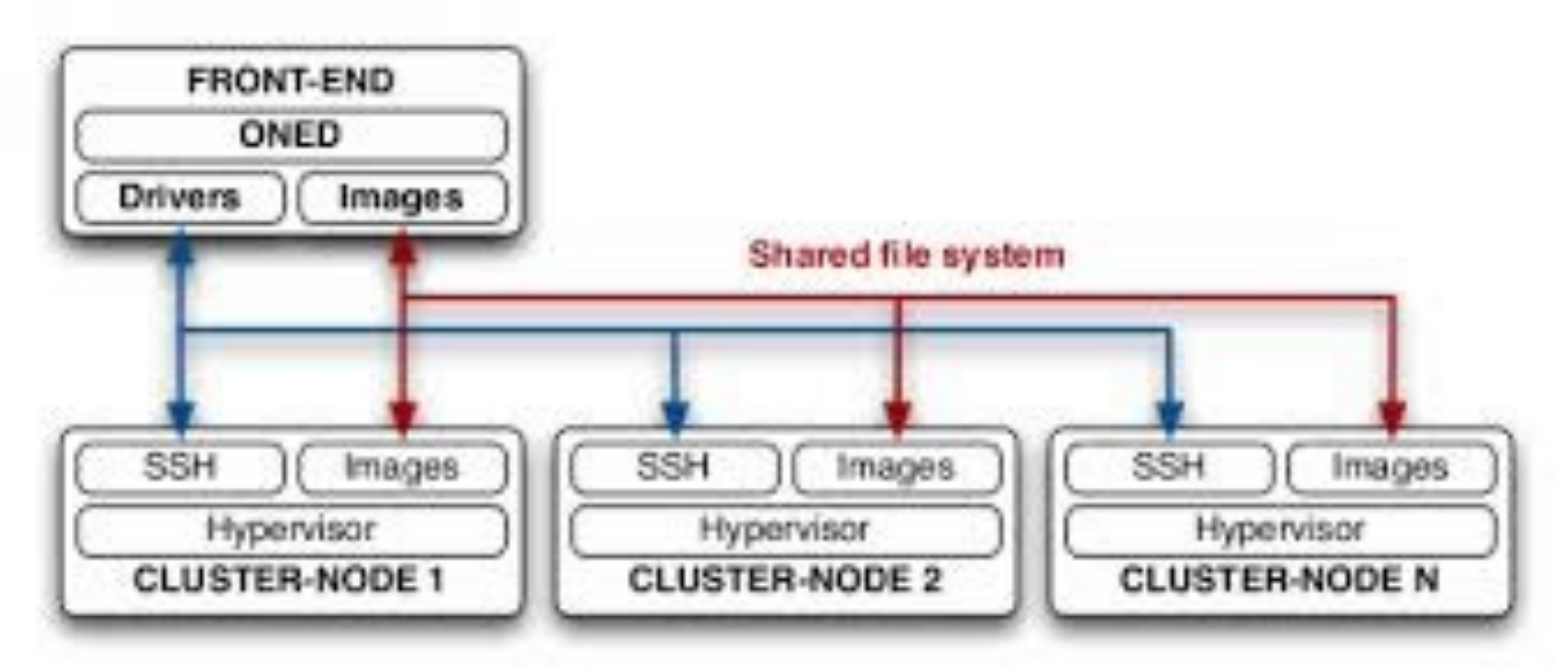
- Opennebula (星雲)
  - Server:29 node
  - CPU:1016 核心
  - MEMORY: 1792 G
  - 壓測:512M 1500台
- OpenStack
  - 6 node
  - CPU:288 核心
  - MEMORY:384 G

平台架構介紹

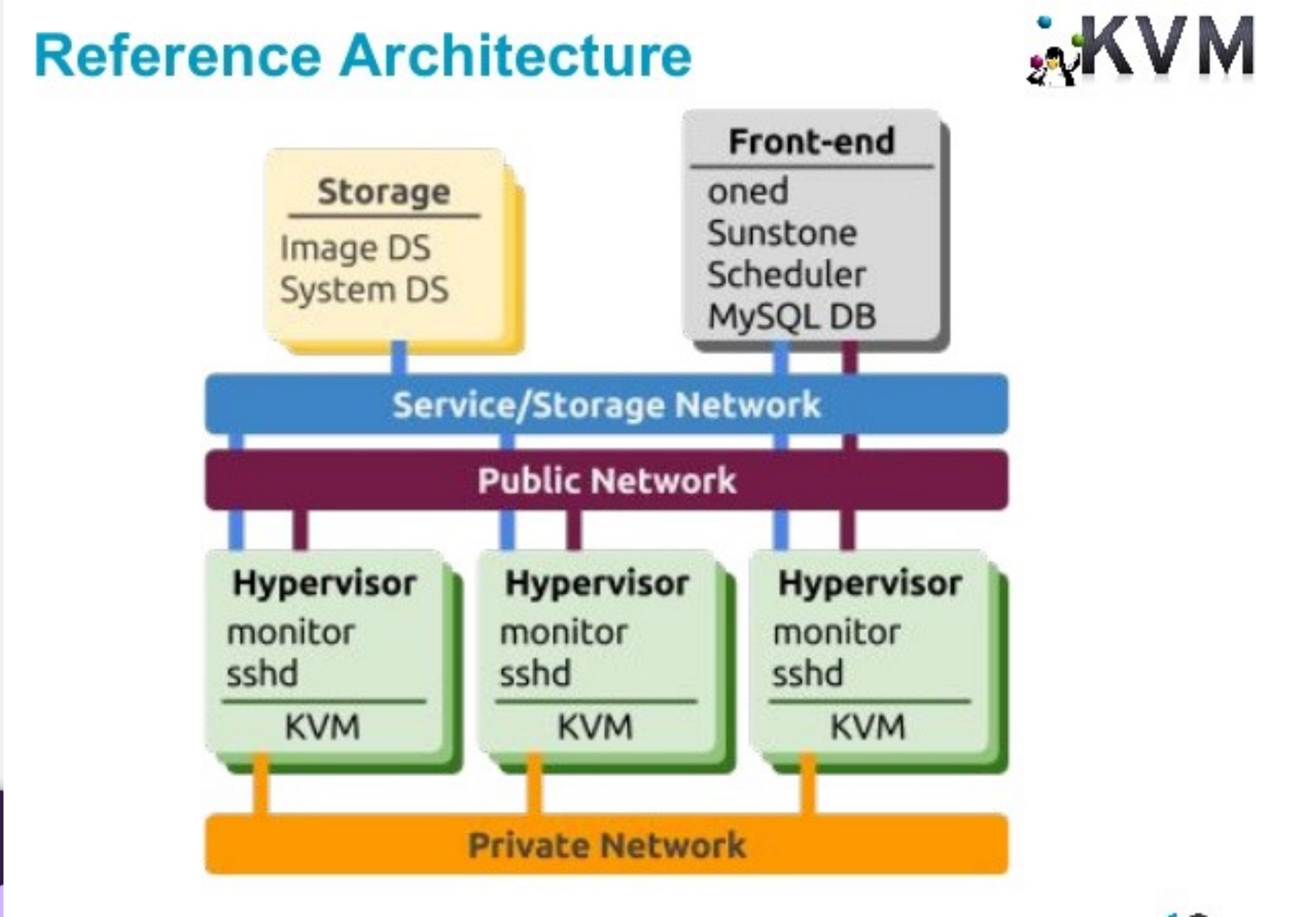

Simplicity
OpenNebula
VM
VM
VM
VM
Hypervisor
Physical Hardware
Host
VM
VM
VM
VM
Hypervisor
Physical Hardware
Host

平台架構介紹

- Front-end 就是 CDX 平台的網頁操作介面
- ONED 使用者碰不到，但實際上是控制所有 host 的程式
- host 是 cluster 中的 node，所以又會叫它 node
- hypervisor 有 KVM、VMware、virtuxlbox、XEN等



平台架構介紹



Reference Architecture

KVM

Storage

Image DS
System DS

Front-end

oned
Sunstone
Scheduler
MySQL DB

Service/Storage Network

Public Network

Hypervisor

monitor
sshd

KVM

Hypervisor

monitor
sshd

KVM

Hypervisor

monitor
sshd

KVM

Private Network

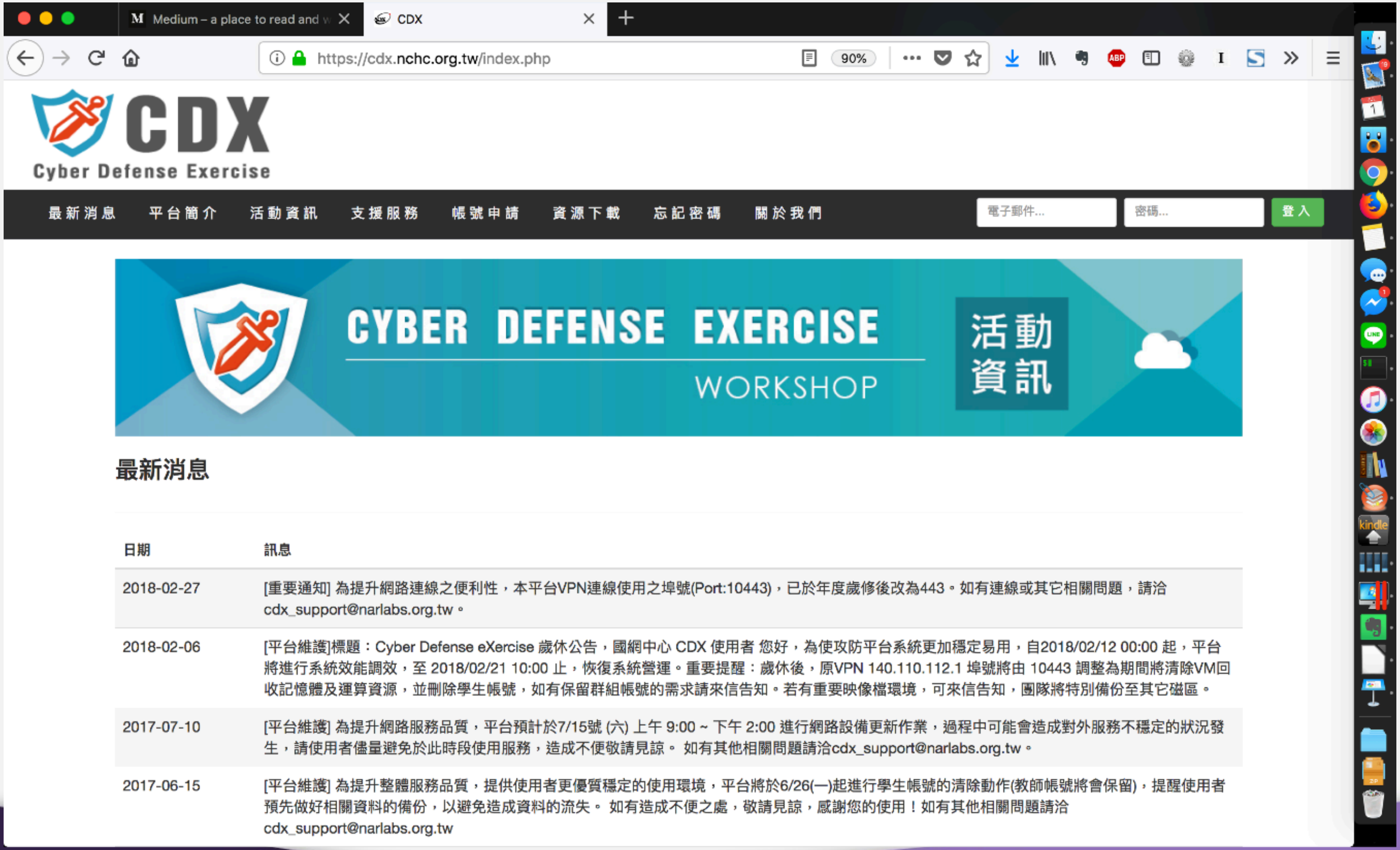
平台架構介紹

- 名詞定義
  - Image-磁碟映像檔
  - Template-範本
    - 用那一個磁碟映像檔
    - 用多少CPU
    - 用多少記憶體
    - 用那一張網路卡
  - VM-Virtual Machine
    - 在Hypervisor上執行中的作業系統
    - 占用系統資源、包含執行中使用的磁碟空間、占用IP、記憶體、CPU
    - 透過Hypervisor 對 VM 關機重開機，連進 console

CDX 攻防平台操作

- 登入方式
- 管理及操作介面
  - 虛擬網路配置
  - CPU及記憶體配置
  - 終端機及遠端桌面
  - 機器固障時
- 軟體元件配置
  - 磁碟映像檔
  - 範本檔
- 操作練習

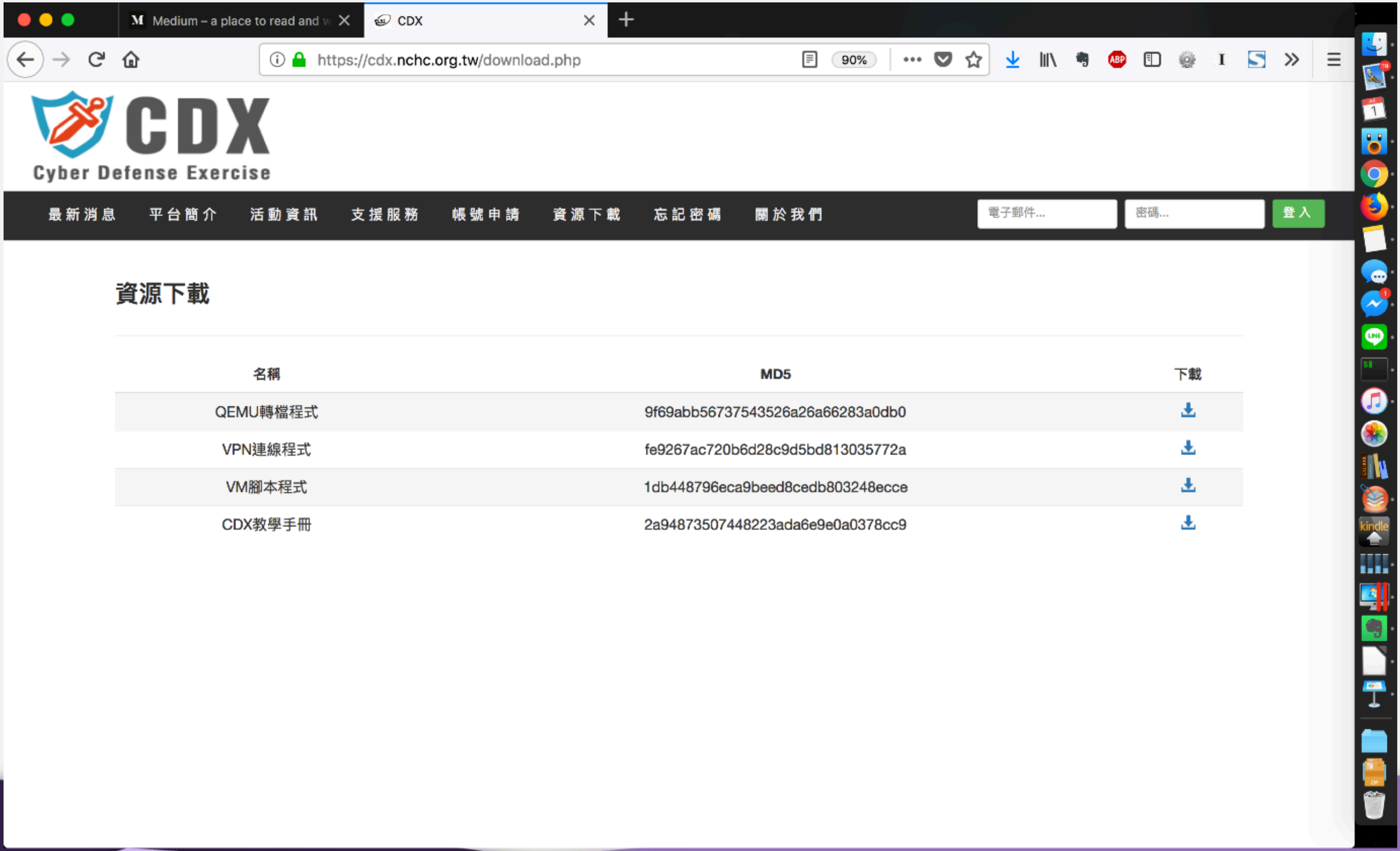
介面操作介紹



最新消息

日期	訊息
2018-02-27	[重要通知] 為提升網路連線之便利性，本平台VPN連線使用之埠號(Port:10443)，已於年度歲修後改為443。如有連線或其它相關問題，請洽cdx_support@narlabs.org.tw。
2018-02-06	[平台維護]標題：Cyber Defense eXercise 歲休公告，國網中心 CDX 使用者 您好，為使攻防平台系統更加穩定易用，自2018/02/12 00:00 起，平台將進行系統效能調效，至 2018/02/21 10:00 止，恢復系統營運。重要提醒：歲休後，原VPN 140.110.112.1 埠號將由 10443 調整為期間將清除VM回收記憶體及運算資源，並刪除學生帳號，如有保留群組帳號的需求請來信告知。若有重要映像檔環境，可來信告知，團隊將特別備份至其它磁區。
2017-07-10	[平台維護] 為提升網路服務品質，平台預計於7/15號 (六) 上午 9:00 ~ 下午 2:00 進行網路設備更新作業，過程中可能會造成對外服務不穩定的狀況發生，請使用者儘量避免於此時段使用服務，造成不便敬請見諒。 如有其他相關問題請洽cdx_support@narlabs.org.tw。
2017-06-15	[平台維護] 為提升整體服務品質，提供使用者更優質穩定的使用環境，平台將於6/26(一)起進行學生帳號的清除動作(教師帳號將會保留)，提醒使用者預先做好相關資料的備份，以避免造成資料的流失。 如有造成不便之處，敬請見諒，感謝您的使用！如有其他相關問題請洽cdx_support@narlabs.org.tw

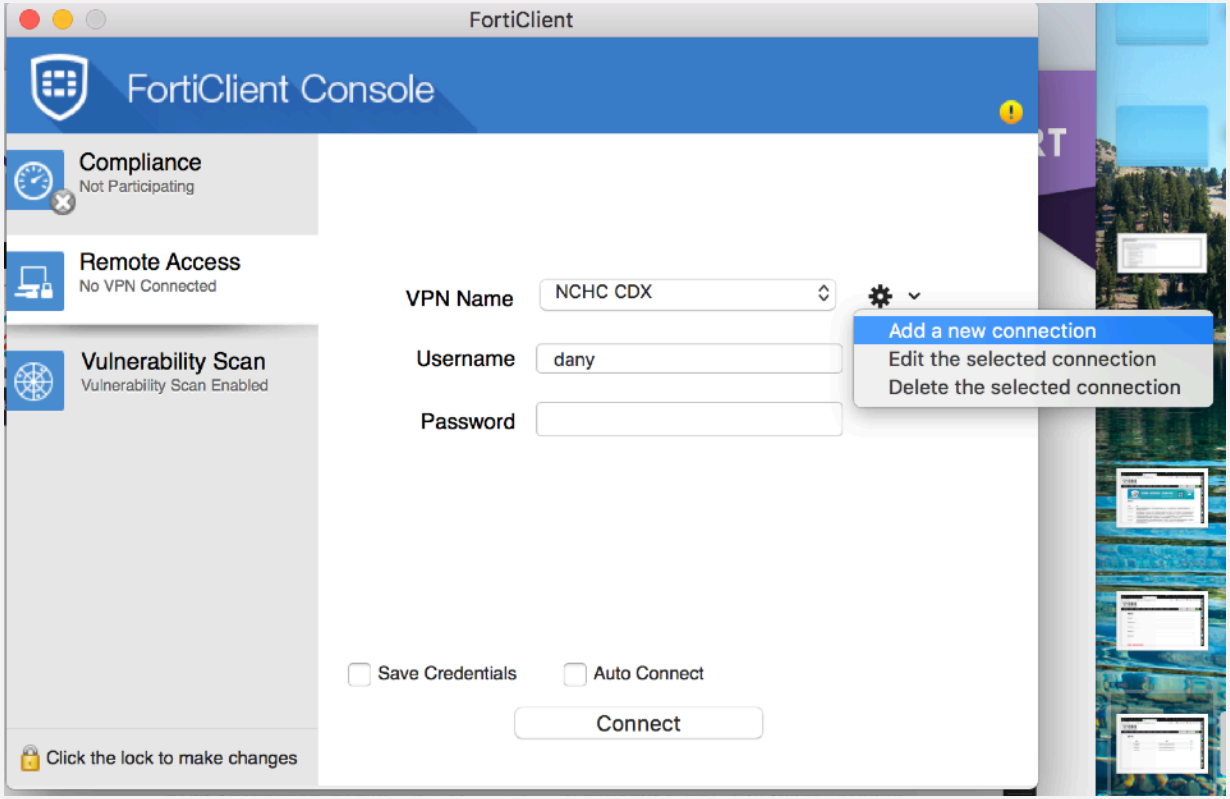
介面操作介紹



資源下載

名稱	MD5	下載
QEMU轉檔程式	9f69abb56737543526a26a66283a0db0	⭳
VPN連線程式	fe9267ac720b6d28c9d5bd813035772a	⭳
VM腳本程式	1db448796eca9beed8cedb803248ecce	⭳
CDX教學手冊	2a94873507448223ada6e9e0a0378cc9	⭳

介面操作介紹



FortiClient

FortiClient Console

Compliance
Not Participating

Remote Access
No VPN Connected

Vulnerability Scan
Vulnerability Scan Enabled

VPN Name: NCHC CDX

Username: dany

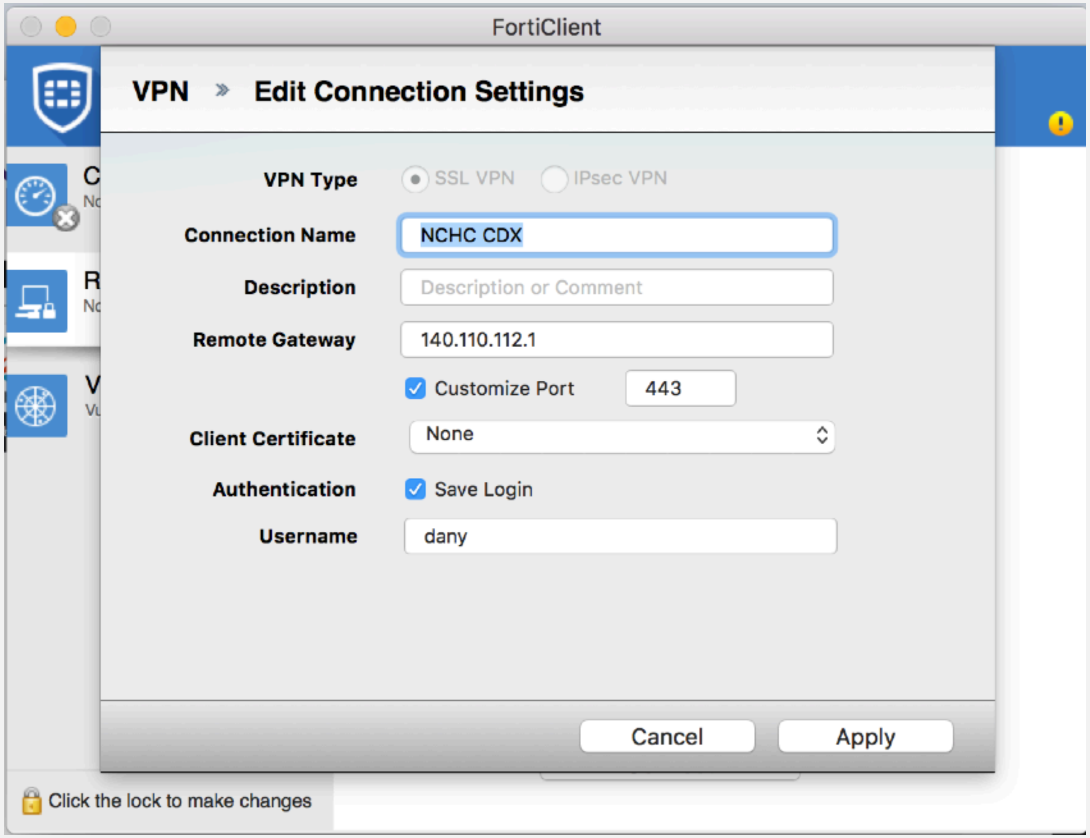
Password:

Add a new connection
Edit the selected connection
Delete the selected connection

□ Save Credentials □ Auto Connect

Connect
Click the lock to make changes

介面操作介紹



FortiClient
VPN » Edit Connection Settings

VPN Type ● SSL VPN ○ IPsec VPN

Connection Name: NCHC CDX

Description: Description or Comment

Remote Gateway: 140.110.112.1

☑ Customize Port: 443

Client Certificate: None

Authentication: ☑ Save Login

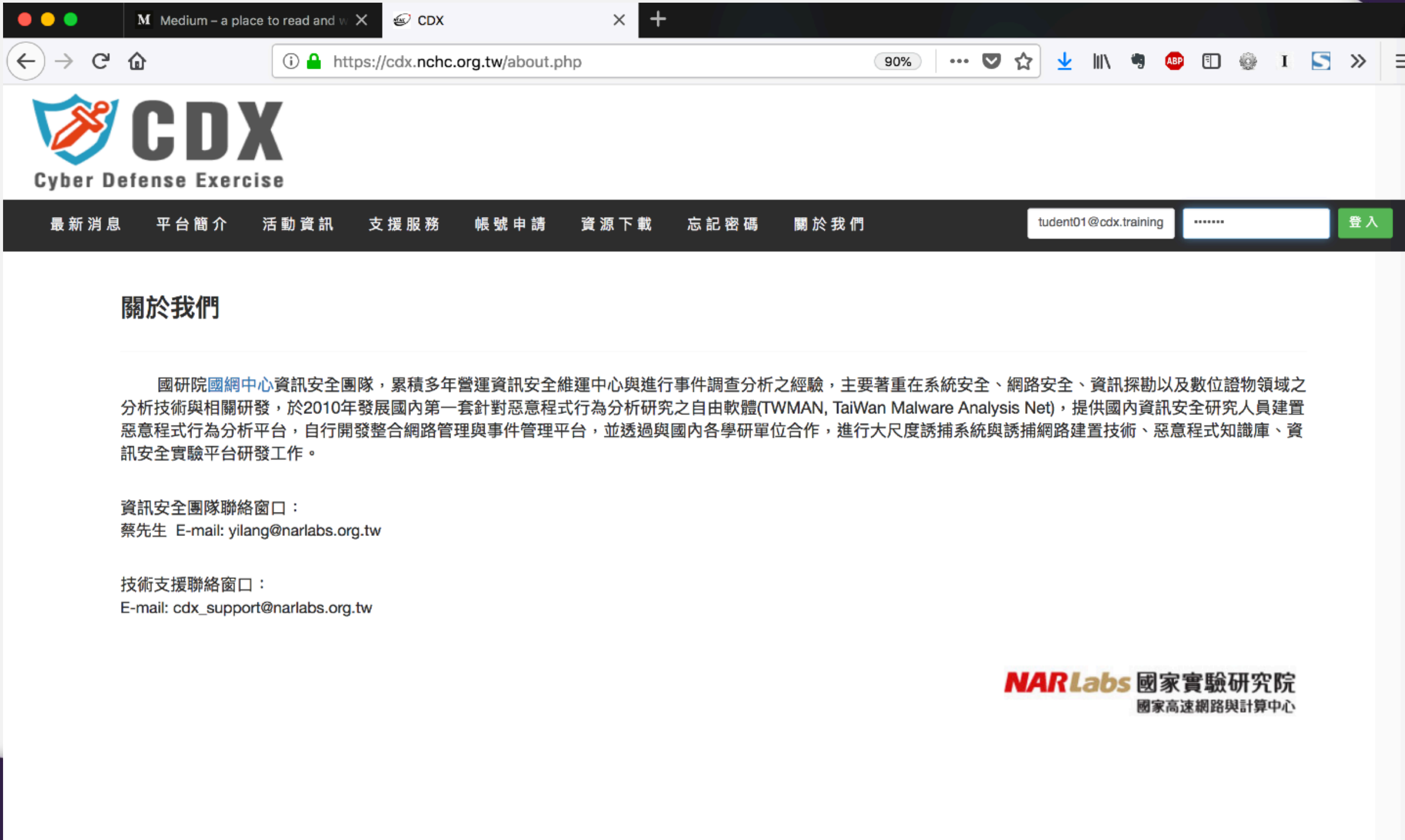
Username: dany

Cancel
Apply
Click the lock to make changes

介面操作介紹

- VPN 連線
  - remote gateway:140.110.112.1
  - 帳號:student01@cdx.training
  - 密碼:npa@cdx
- 第一步 VPN 連線
  - 方式1:登入 CDX 網頁再登入 CDX 平台
  - 方式2:直接登入CDX 平台
    - http://192.168.66.160:9869/

介面操作介紹



關於我們

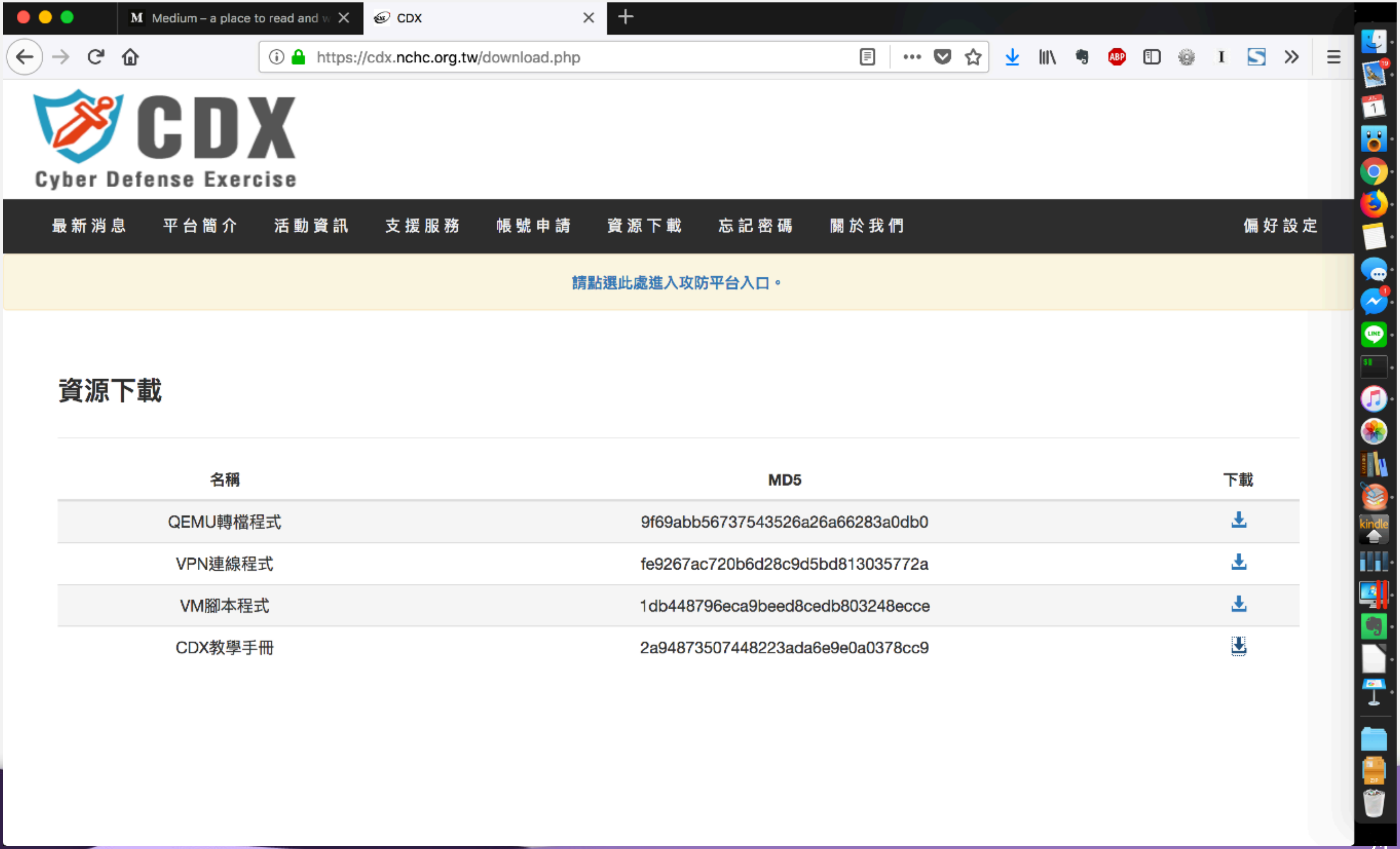
國研院國網中心資訊安全團隊，累積多年營運資訊安全維運中心與進行事件調查分析之經驗，主要著重在系統安全、網路安全、資訊探勘以及數位證物領域之分析技術與相關研發，於2010年發展國內第一套針對惡意程式行為分析研究之自由軟體(TWMAN, TaiWan Malware Analysis Net)，提供國內資訊安全研究人員建置惡意程式行為分析平台，自行開發整合網路管理與事件管理平台，並透過與國內各學研單位合作，進行大尺度誘捕系統與誘捕網路建置技術、惡意程式知識庫、資訊安全實驗平台研發工作。

資訊安全團隊聯絡窗口：
蔡先生 E-mail: yilang@narlabs.org.tw

技術支援聯絡窗口：
E-mail: cdx_support@narlabs.org.tw

NARLabs 國家實驗研究院
國家高速網路與計算中心

介面操作介紹

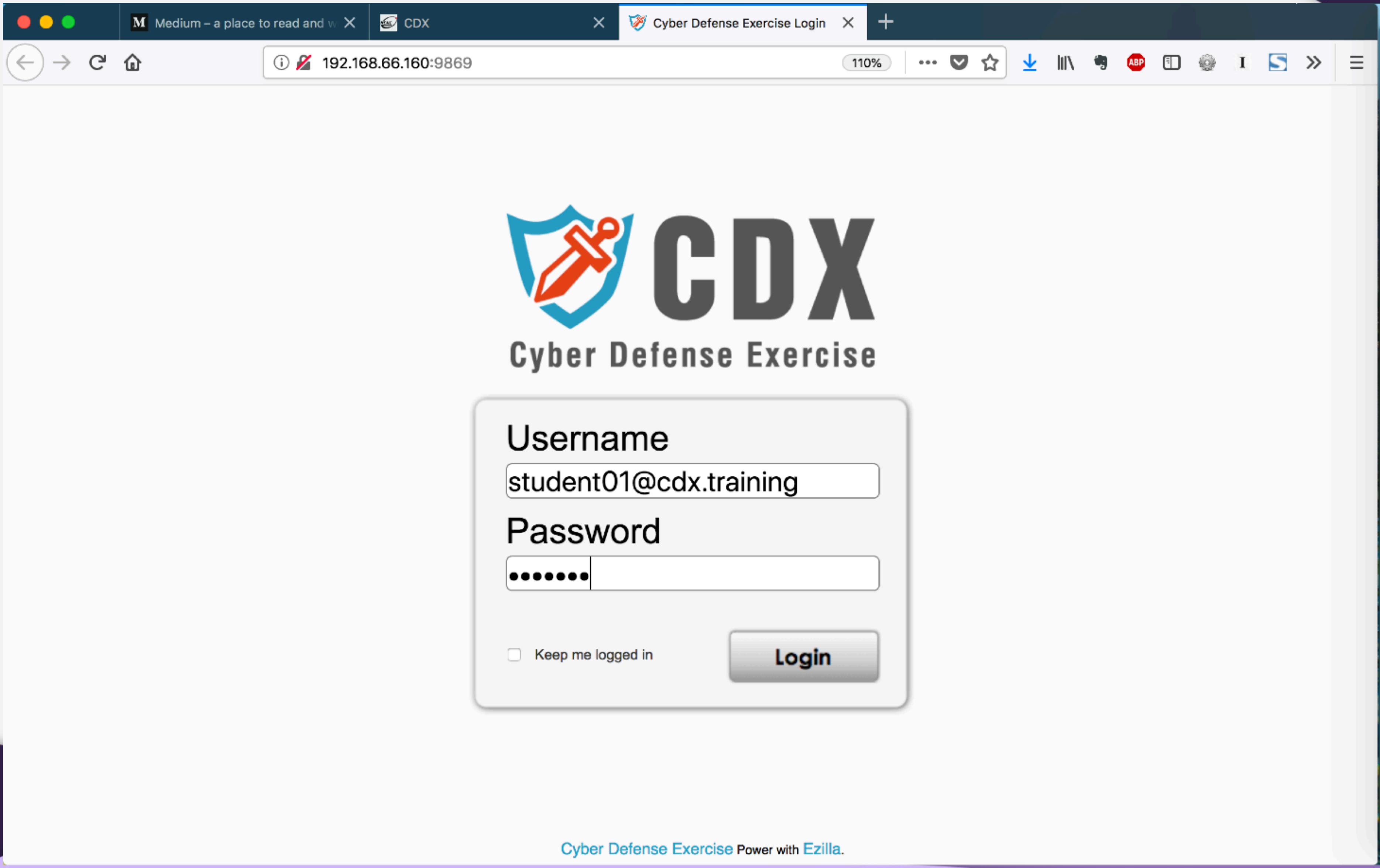


請點選此處進入攻防平台入口。

資源下載

名稱	MD5	下載
QEMU轉檔程式	9f69abb56737543526a26a66283a0db0	⤓
VPN連線程式	fe9267ac720b6d28c9d5bd813035772a	⤓
VM腳本程式	1db448796eca9beed8cedb803248ecce	⤓
CDX教學手冊	2a94873507448223ada6e9e0a0378cc9	⤓

介面操作介紹



Username

student01@cdx.training

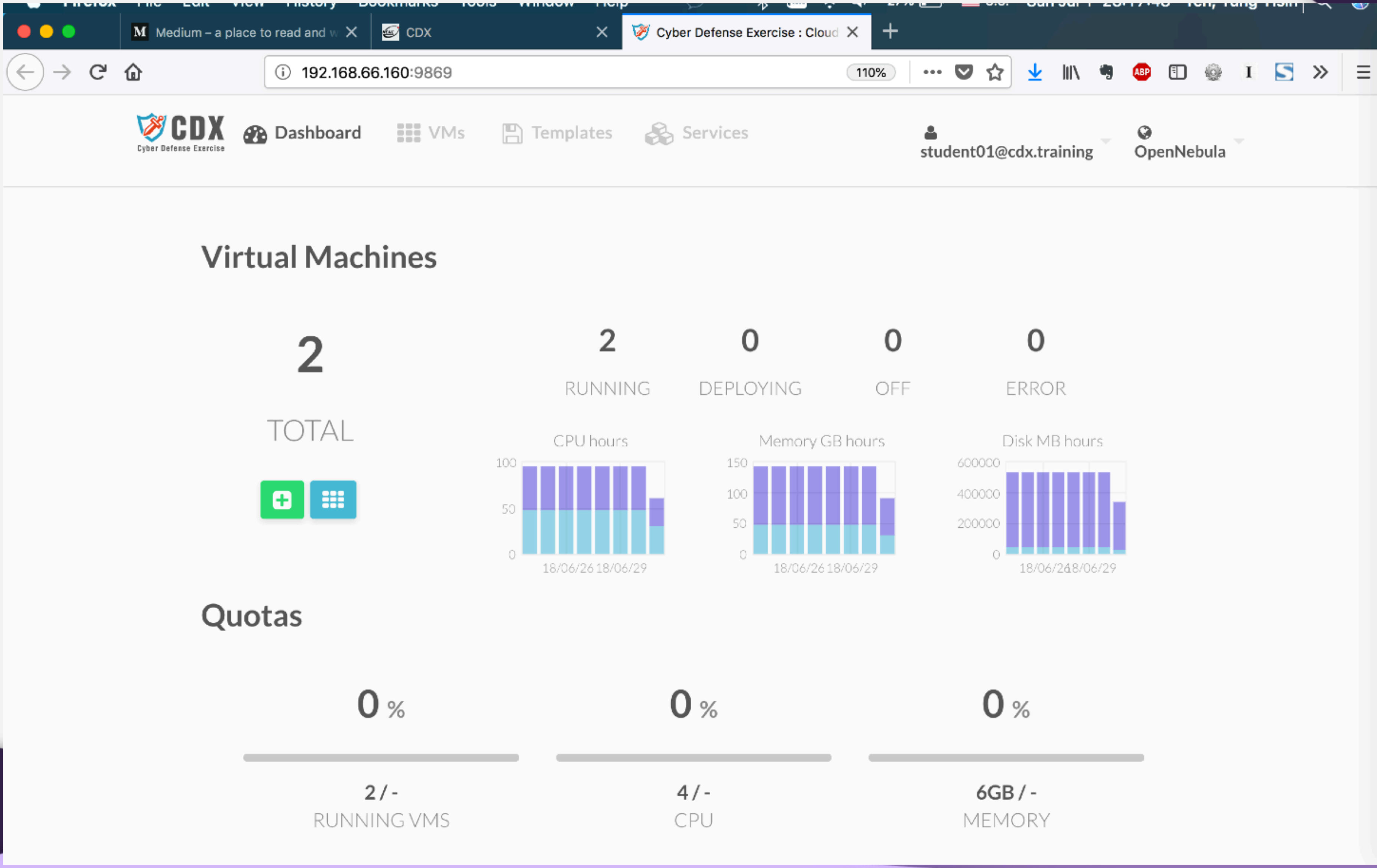
Password

●●●●●●●

□ Keep me logged in

Cyber Defense Exercise Power with Ezilla.

介面操作介紹



Virtual Machines

2 TOTAL

2 RUNNING

0 DEPLOYING

0 OFF

0 ERROR

Quotas

0 %

2 / -
RUNNING VMS

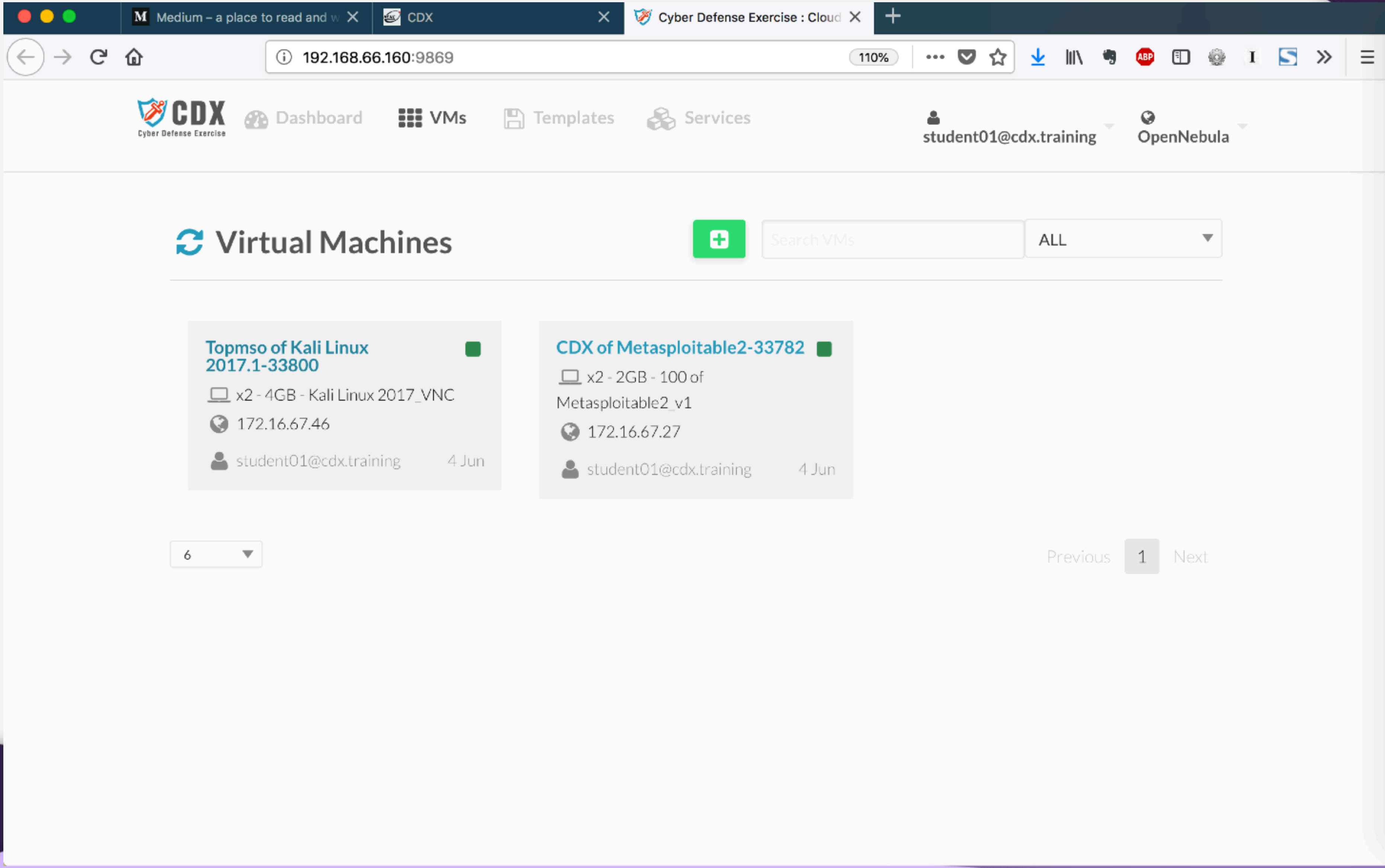
0 %

4 / -
CPU

0 %

6GB / -
MEMORY

介面操作介紹

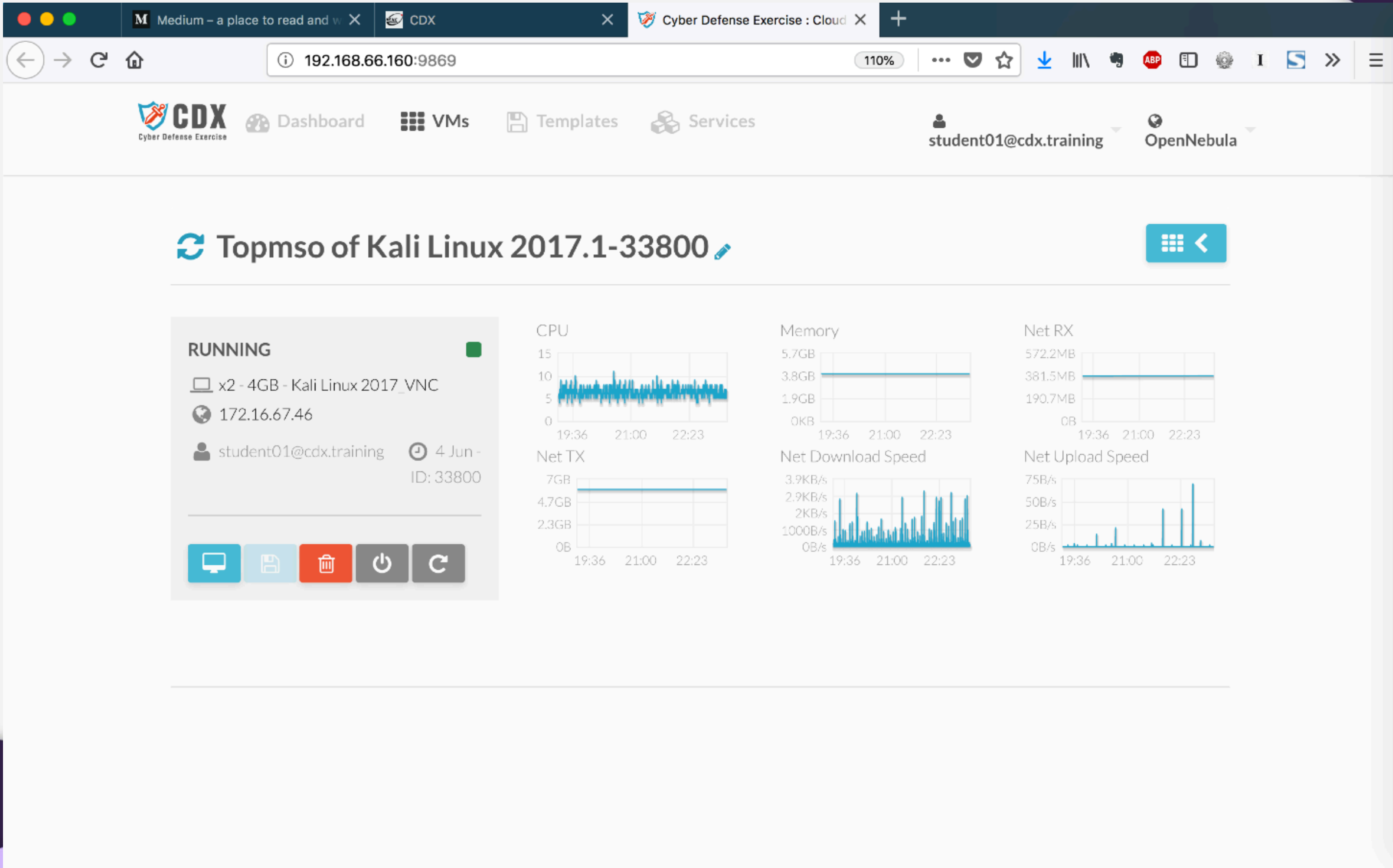


Virtual Machines

Topmso of Kali Linux 2017.1-33800 🟩
x2 - 4GB - Kali Linux 2017_VNC
172.16.67.46
student01@cdx.training 4 Jun

CDX of Metasploitable2-33782 🟩
x2 - 2GB - 100 of Metasploitable2_v1
172.16.67.27
student01@cdx.training 4 Jun

介面操作介紹



Topmso of Kali Linux 2017.1-33800

RUNNING 🟩

x2 - 4GB - Kali Linux 2017_VNC

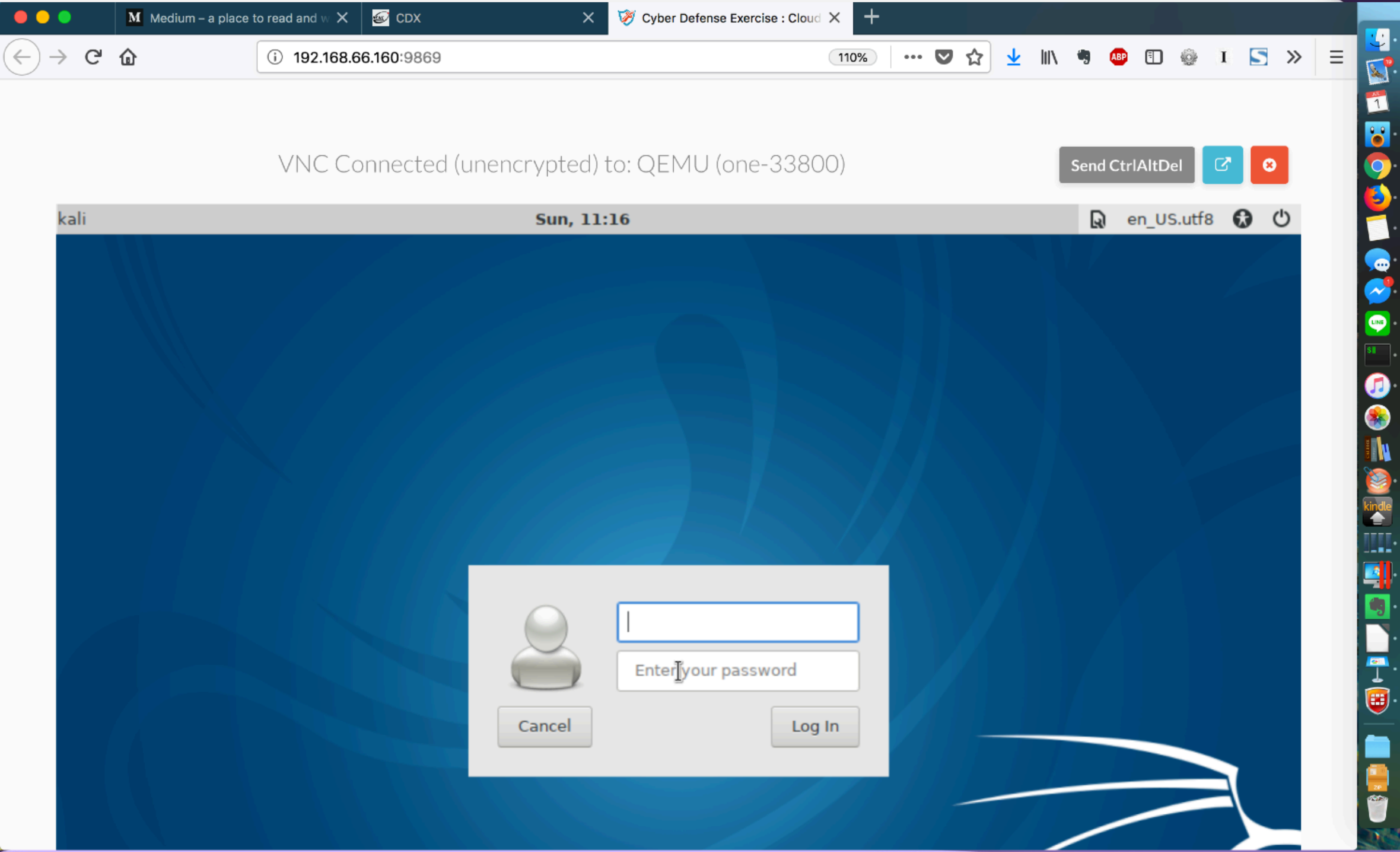
172.16.67.46

student01@cdx.training

4 Jun -

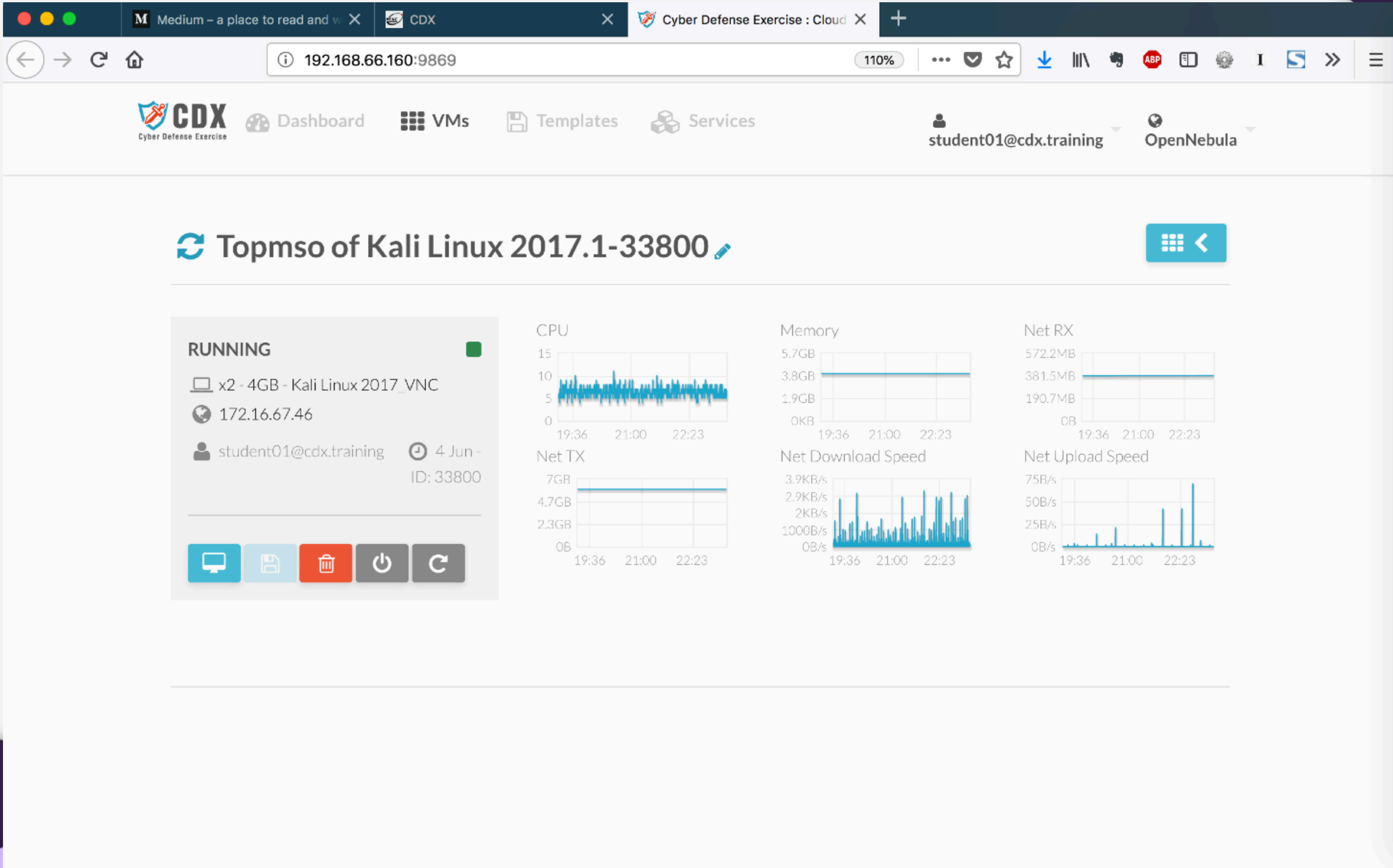
ID: 33800

介面操作介紹



VNC Connected (unencrypted) to: QEMU (one-33800)

介面操作介紹



Topmso of Kali Linux 2017.1-33800

RUNNING 🟩

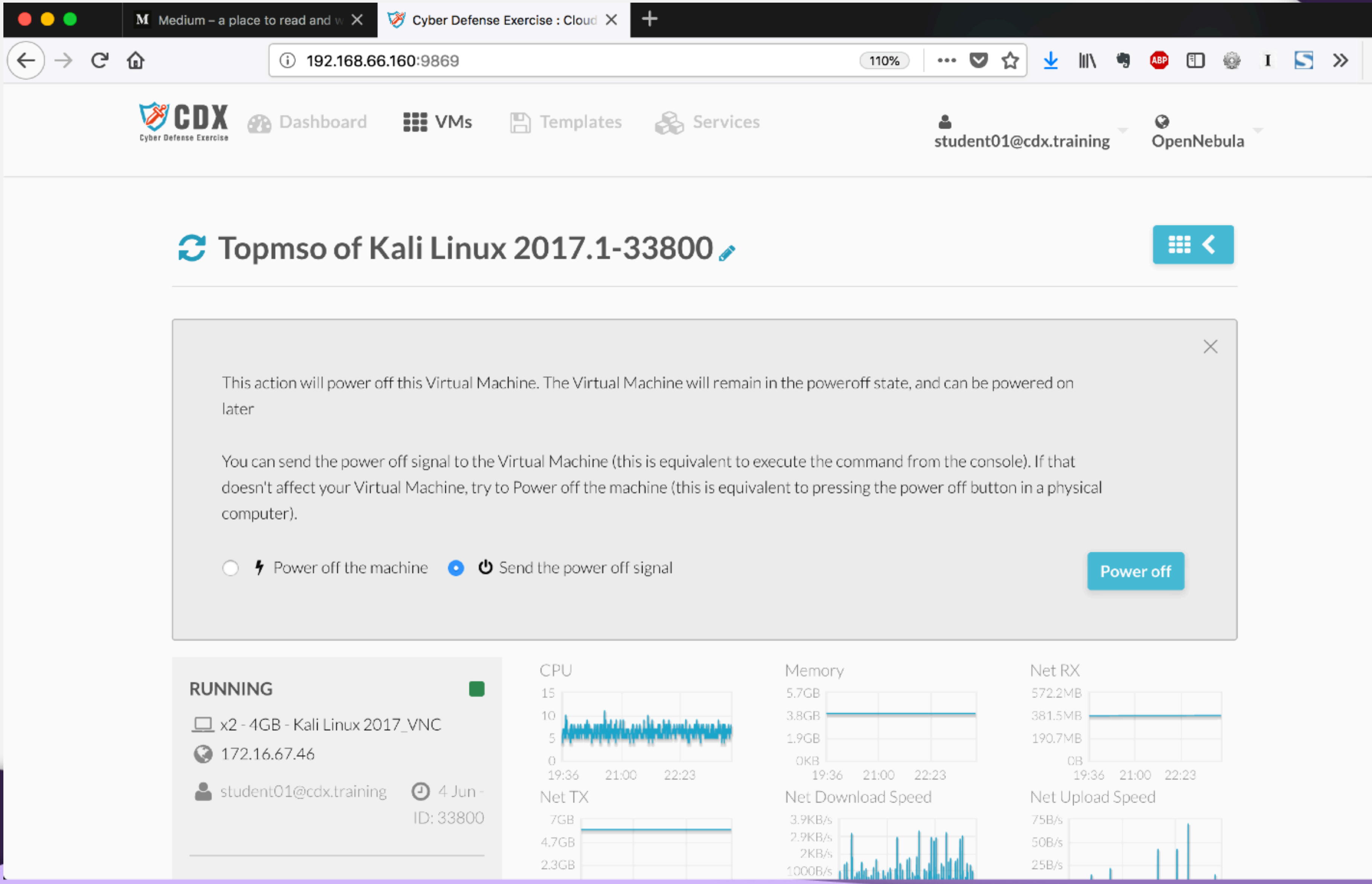
x2 - 4GB - Kali Linux 2017_VNC

172.16.67.46

student01@cdx.training 4 Jun -

ID: 33800

介面操作介紹



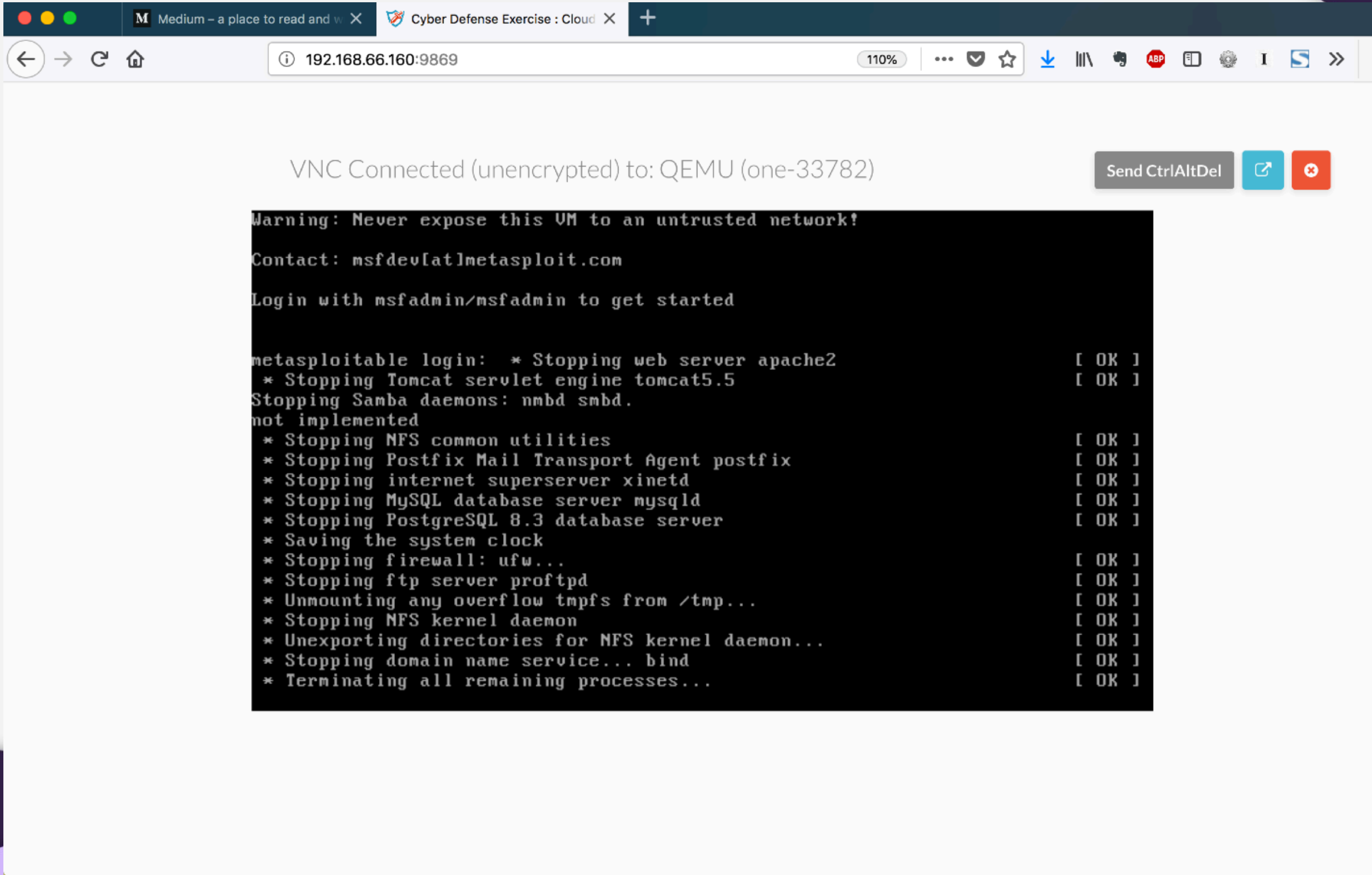
Topmso of Kali Linux 2017.1-33800

This action will power off this Virtual Machine. The Virtual Machine will remain in the poweroff state, and can be powered on later

You can send the power off signal to the Virtual Machine (this is equivalent to execute the command from the console). If that doesn't affect your Virtual Machine, try to Power off the machine (this is equivalent to pressing the power off button in a physical computer).

○ Power off the machine ● Send the power off signal

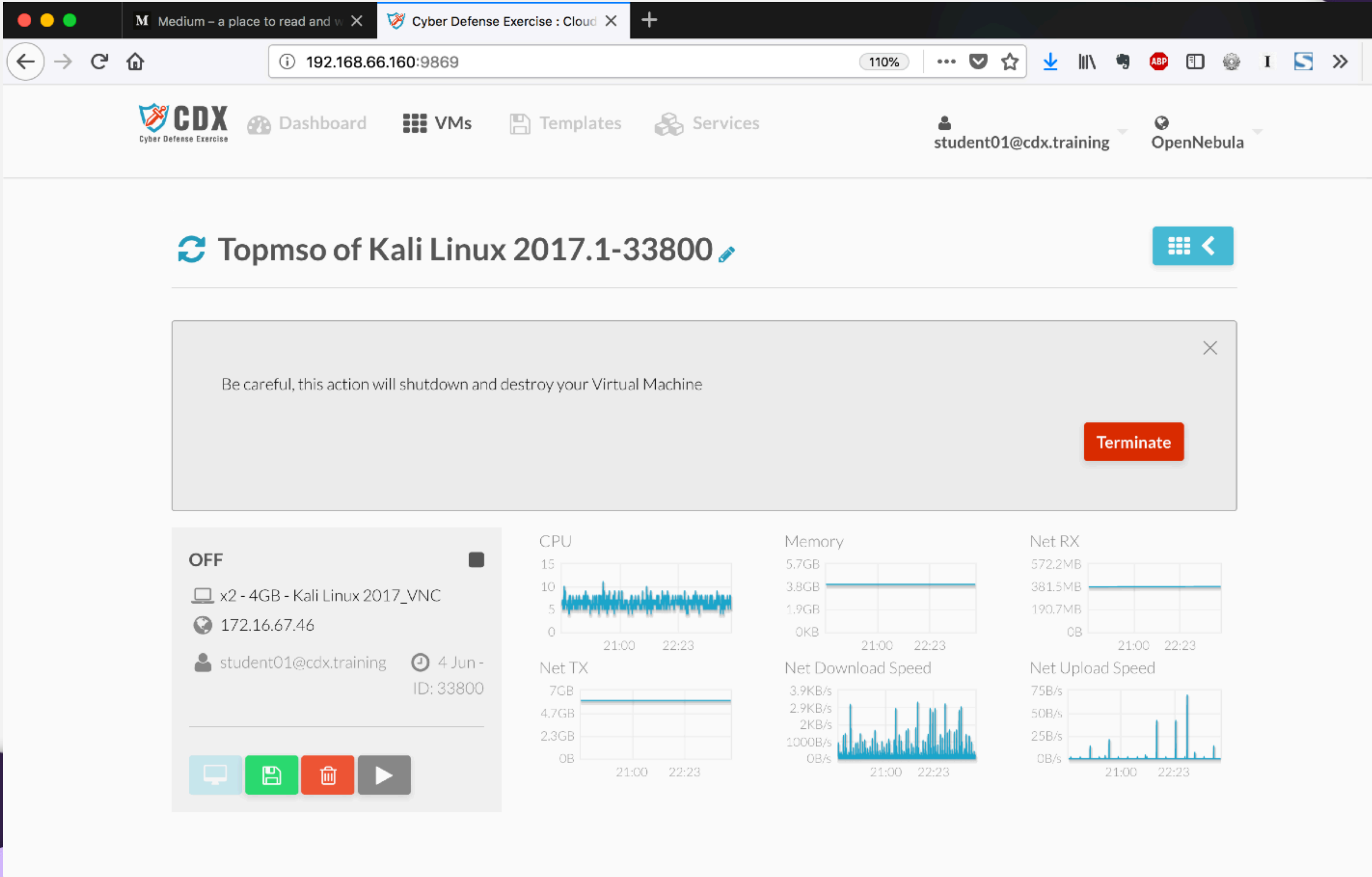
介面操作介紹


Medium – a place to read and w
Cyber Defense Exercise : Cloud
192.168.66.160:9869
110%
Send CtrlAltDel

VNC Connected (unencrypted) to: QEMU (one-33782)

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:  * Stopping web server apache2                     [ OK ]
 * Stopping Tomcat servlet engine tomcat5.5                              [ OK ]
Stopping Samba daemons: nmbd smbd.
not implemented
 * Stopping NFS common utilities                                          [ OK ]
 * Stopping Postfix Mail Transport Agent postfix                          [ OK ]
 * Stopping internet superserver xinetd                                   [ OK ]
 * Stopping MySQL database server mysqld                                  [ OK ]
 * Stopping PostgreSQL 8.3 database server                                [ OK ]
 * Saving the system clock
 * Stopping firewall: ufw...                                              [ OK ]
 * Stopping ftp server proftpd                                            [ OK ]
 * Unmounting any overflow tmpfs from /tmp...                             [ OK ]
 * Stopping NFS kernel daemon                                             [ OK ]
 * Unexporting directories for NFS kernel daemon...                       [ OK ]
 * Stopping domain name service... bind                                   [ OK ]
 * Terminating all remaining processes...                                 [ OK ]
```

介面操作介紹



Topmso of Kali Linux 2017.1-33800

Be careful, this action will shutdown and destroy your Virtual Machine

OFF

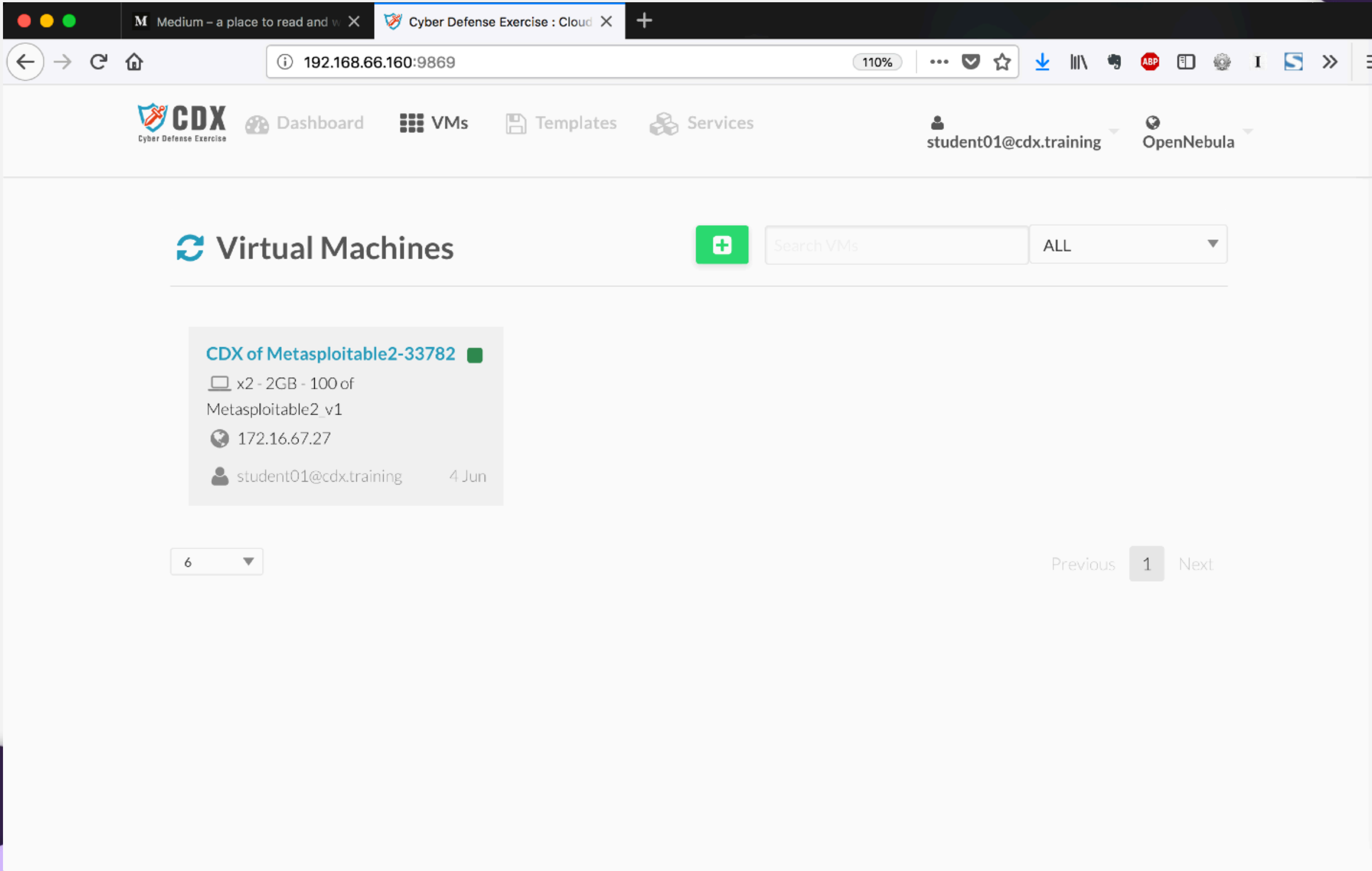
x2 - 4GB - Kali Linux 2017_VNC

172.16.67.46

student01@cdx.training 4 Jun -

ID: 33800

介面操作介紹



Virtual Machines

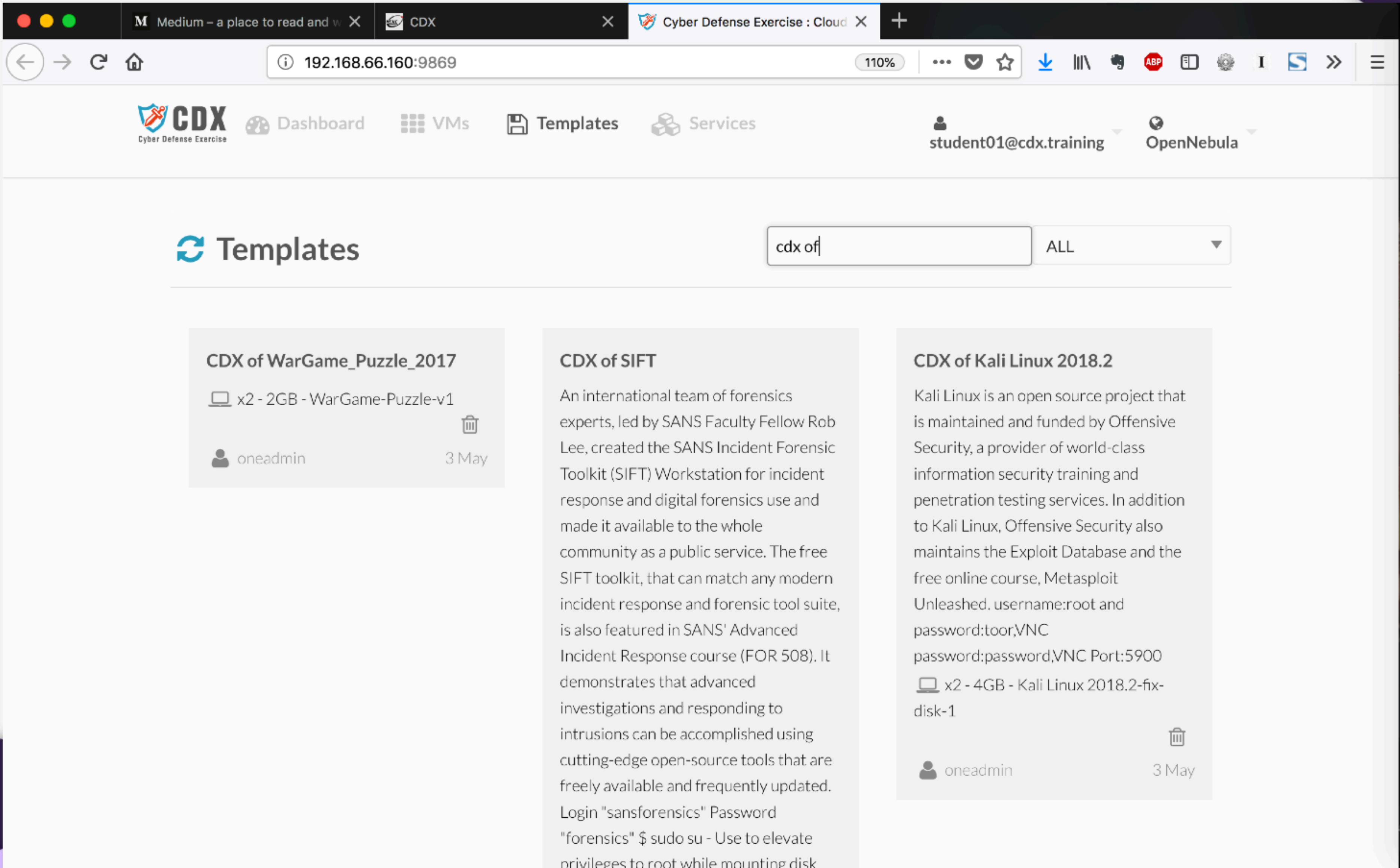
CDX of Metasploitable2-33782 🟩

x2 - 2GB - 100 of Metasploitable2_v1

172.16.67.27

student01@cdx.training 4 Jun

介面操作介紹



Templates

cdx of

ALL

CDX of WarGame_Puzzle_2017

x2 - 2GB - WarGame-Puzzle-v1

oneadmin 3 May

CDX of SIFT

An international team of forensics experts, led by SANS Faculty Fellow Rob Lee, created the SANS Incident Forensic Toolkit (SIFT) Workstation for incident response and digital forensics use and made it available to the whole community as a public service. The free SIFT toolkit, that can match any modern incident response and forensic tool suite, is also featured in SANS' Advanced Incident Response course (FOR 508). It demonstrates that advanced investigations and responding to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated. Login "sansforensics" Password "forensics" $ sudo su - Use to elevate privileges to root while mounting disk

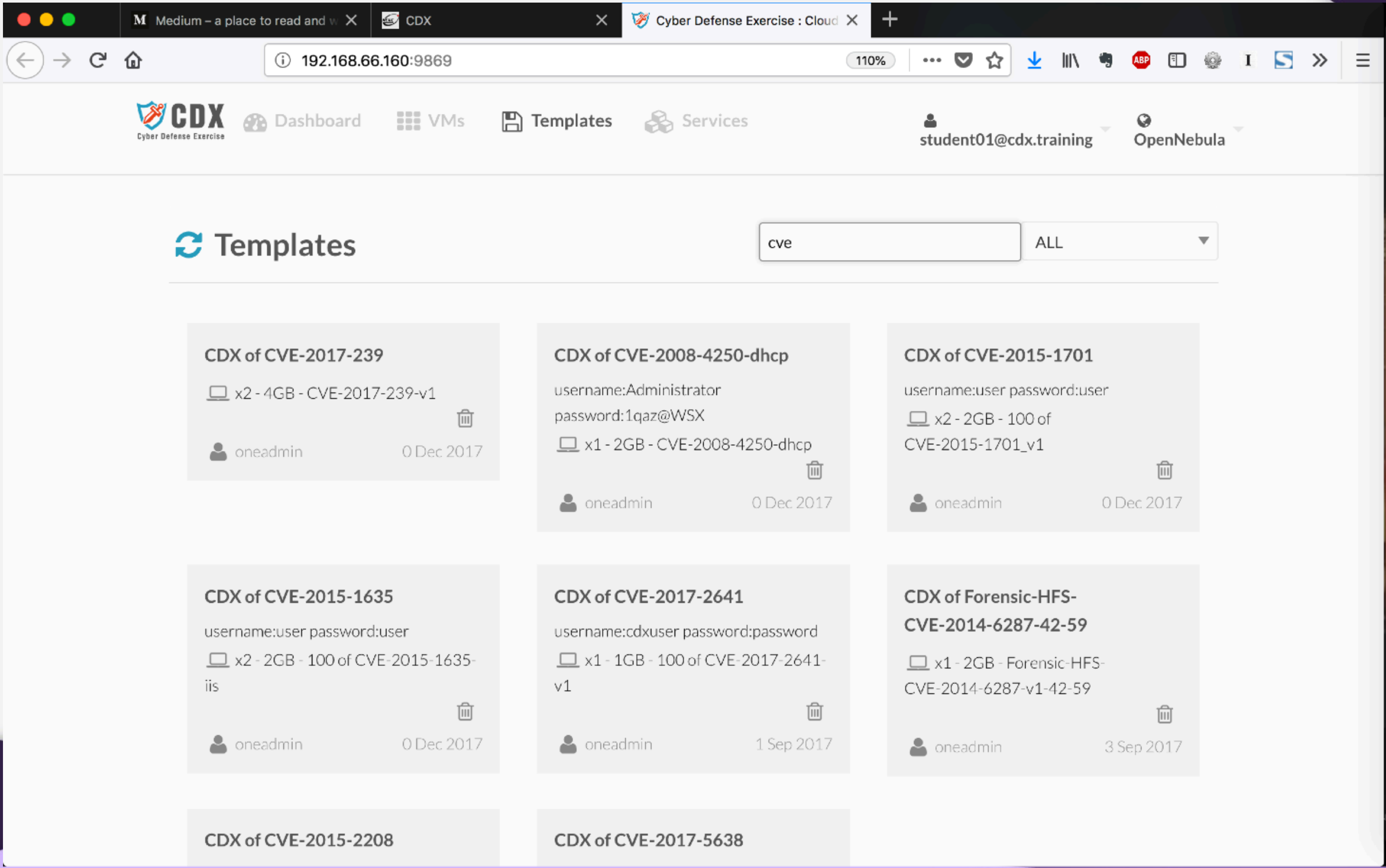
CDX of Kali Linux 2018.2

Kali Linux is an open source project that is maintained and funded by Offensive Security, a provider of world-class information security training and penetration testing services. In addition to Kali Linux, Offensive Security also maintains the Exploit Database and the free online course, Metasploit Unleashed. username:root and password:toor,VNC password:password,VNC Port:5900

x2 - 4GB - Kali Linux 2018.2-fix-disk-1

oneadmin 3 May

介面操作介紹



Templates

cve

ALL

CDX of CVE-2017-239

x2 - 4GB - CVE-2017-239-v1

oneadmin 0 Dec 2017

CDX of CVE-2008-4250-dhcp

username:Administrator password:1qaz@WSX

x1 - 2GB - CVE-2008-4250-dhcp

oneadmin 0 Dec 2017

CDX of CVE-2015-1701

username:user password:user

x2 - 2GB - 100 of CVE-2015-1701_v1

oneadmin 0 Dec 2017

CDX of CVE-2015-1635

username:user password:user

x2 - 2GB - 100 of CVE-2015-1635-iis

oneadmin 0 Dec 2017

CDX of CVE-2017-2641

username:cdxuser password:password

x1 - 1GB - 100 of CVE-2017-2641-v1

oneadmin 1 Sep 2017

CDX of Forensic-HFS-CVE-2014-6287-42-59

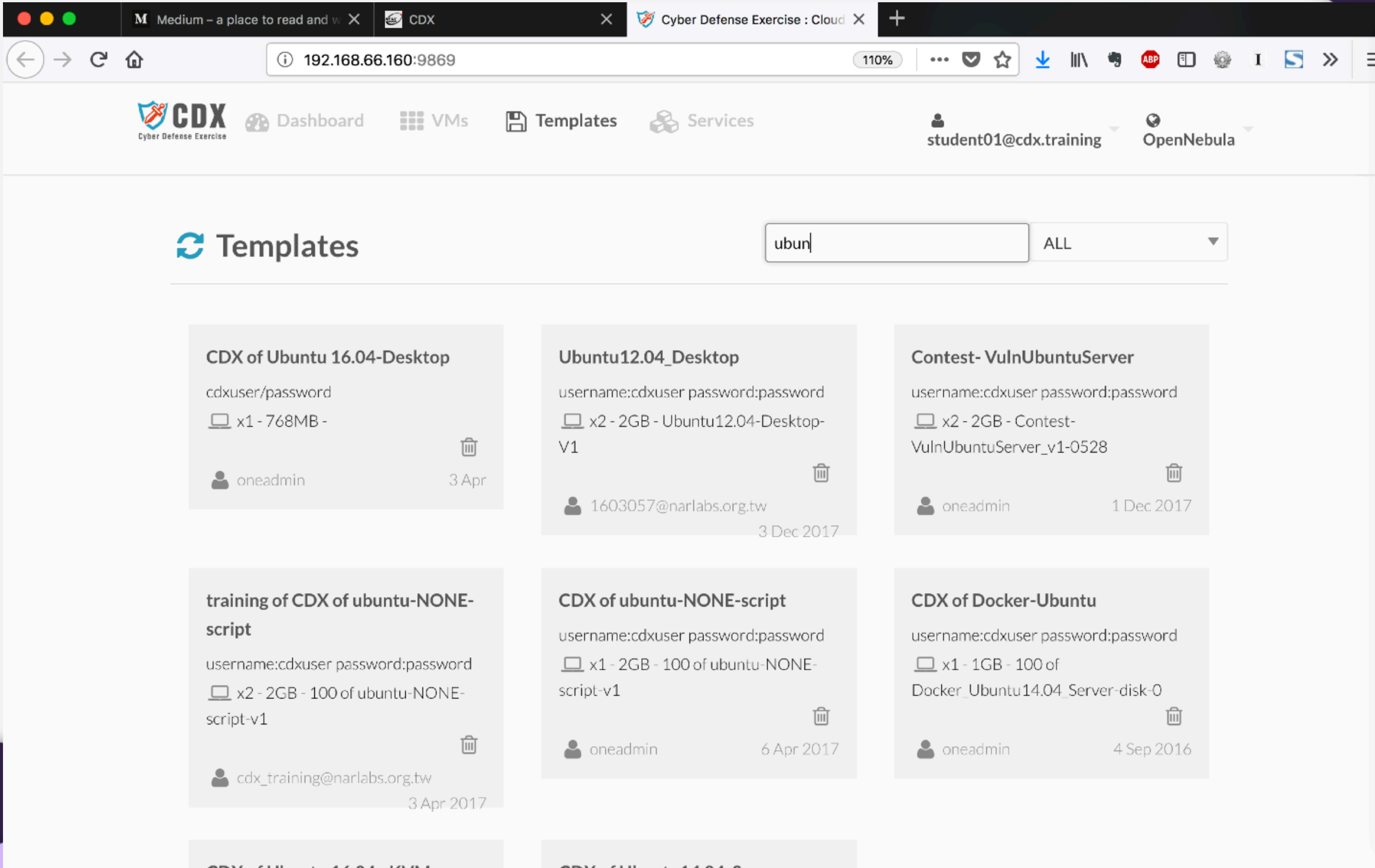
x1 - 2GB - Forensic-HFS-CVE-2014-6287-v1-42-59

oneadmin 3 Sep 2017

CDX of CVE-2015-2208

CDX of CVE-2017-5638

介面操作介紹



Templates

Search: ubun | ALL

CDX of Ubuntu 16.04-Desktop
cdxuser/password
x1 - 768MB -
oneadmin 3 Apr

Ubuntu12.04_Desktop
username:cdxuser password:password
x2 - 2GB - Ubuntu12.04-Desktop-V1
1603057@narlabs.org.tw 3 Dec 2017

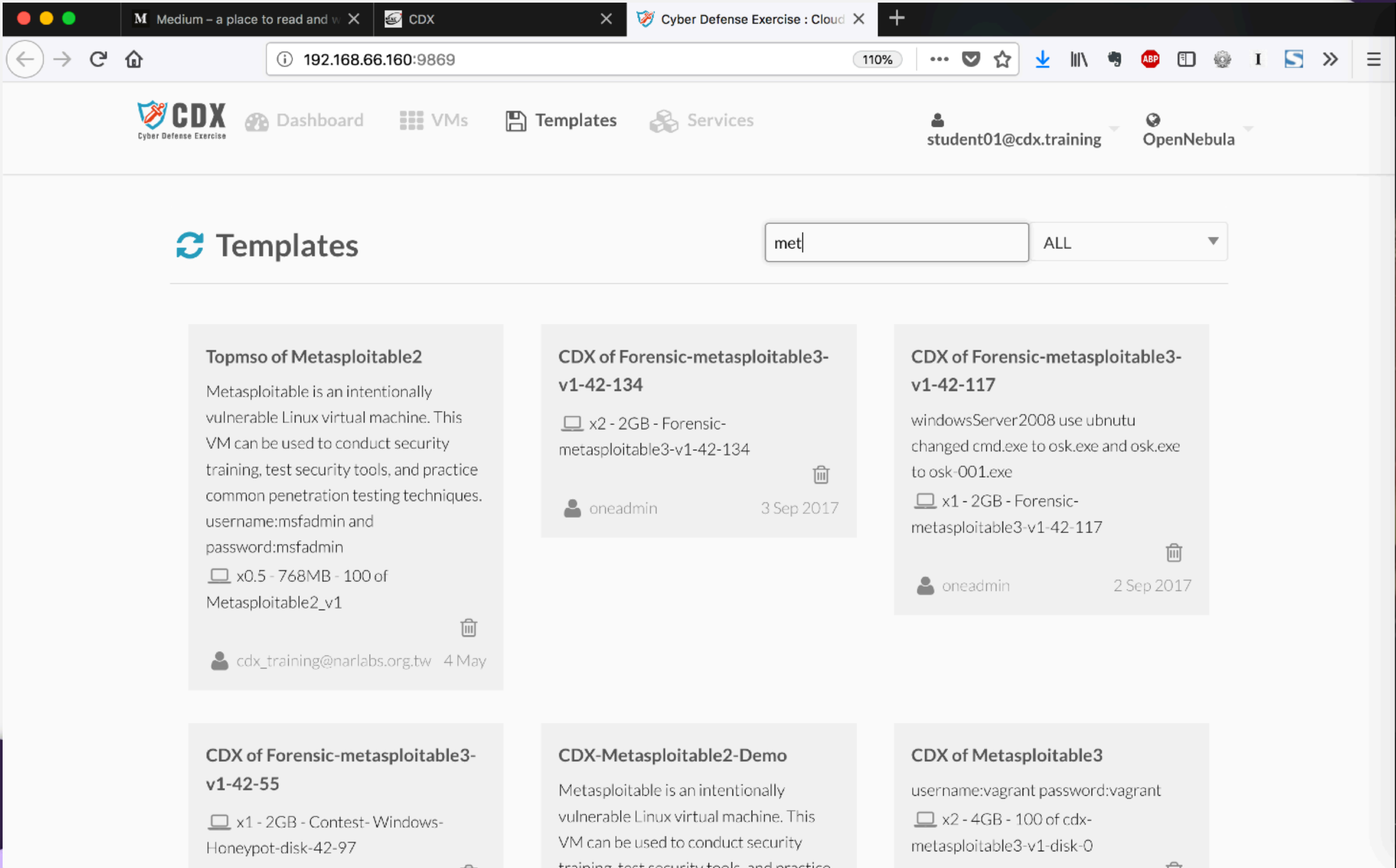
Contest- VulnUbuntuServer
username:cdxuser password:password
x2 - 2GB - Contest-VulnUbuntuServer_v1-0528
oneadmin 1 Dec 2017

training of CDX of ubuntu-NONE-script
username:cdxuser password:password
x2 - 2GB - 100 of ubuntu-NONE-script-v1
cdx_training@narlabs.org.tw 3 Apr 2017

CDX of ubuntu-NONE-script
username:cdxuser password:password
x1 - 2GB - 100 of ubuntu-NONE-script-v1
oneadmin 6 Apr 2017

CDX of Docker-Ubuntu
username:cdxuser password:password
x1 - 1GB - 100 of Docker_Ubuntu14.04_Server-disk-0
oneadmin 4 Sep 2016

介面操作介紹



Templates

met

ALL

Topmso of Metasploitable2

Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques. username:msfadmin and password:msfadmin

x0.5 - 768MB - 100 of Metasploitable2_v1

cdx_training@narlabs.org.tw 4 May

CDX of Forensic-metasploitable3-v1-42-134

x2 - 2GB - Forensic-metasploitable3-v1-42-134

oneadmin 3 Sep 2017

CDX of Forensic-metasploitable3-v1-42-117

windowsServer2008 use ubnutu changed cmd.exe to osk.exe and osk.exe to osk-001.exe

x1 - 2GB - Forensic-metasploitable3-v1-42-117

oneadmin 2 Sep 2017

CDX of Forensic-metasploitable3-v1-42-55

x1 - 2GB - Contest- Windows-Honeypot-disk-42-97

CDX-Metasploitable2-Demo

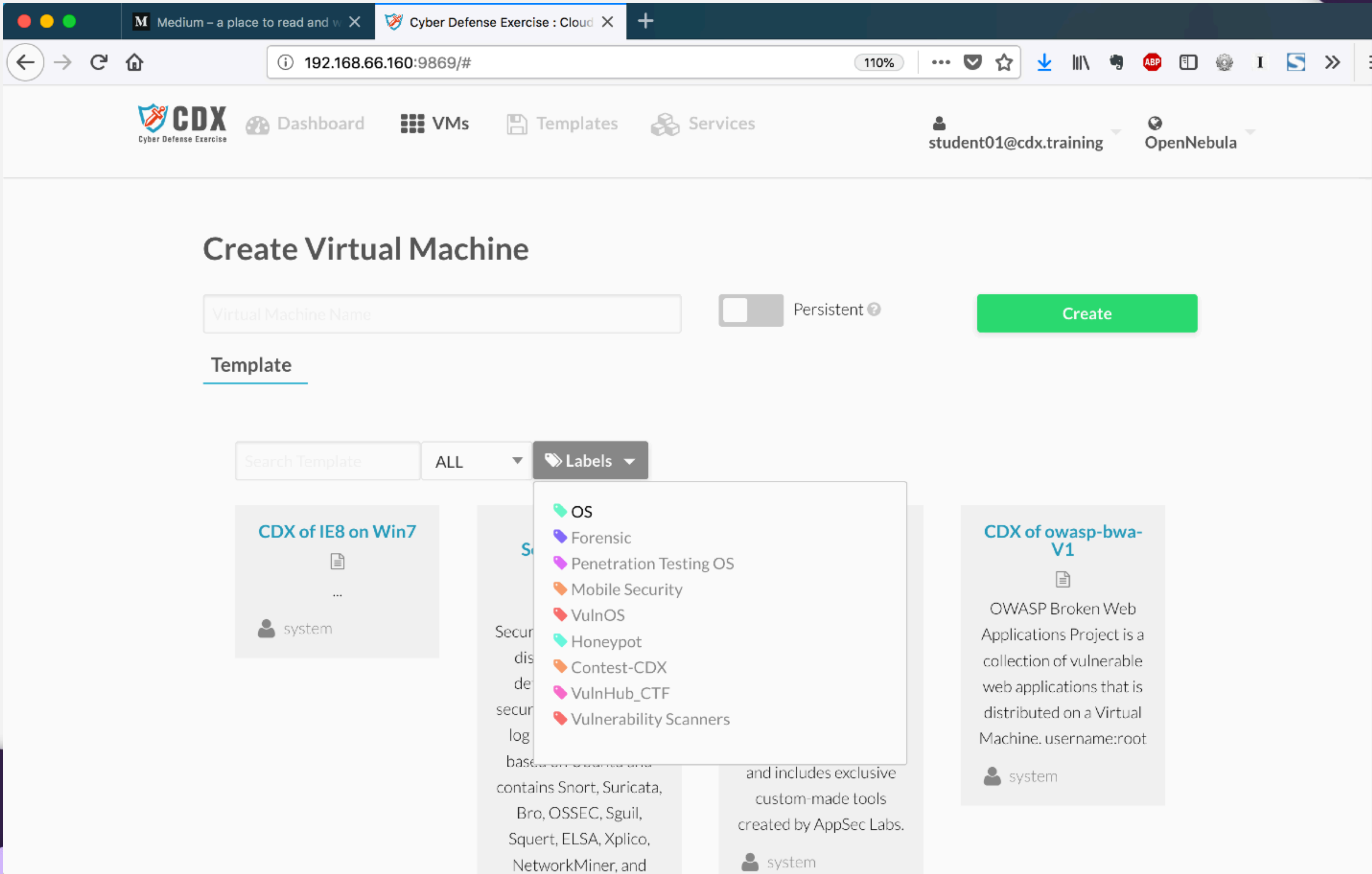
Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice

CDX of Metasploitable3

username:vagrant password:vagrant

x2 - 4GB - 100 of cdx-metasploitable3-v1-disk-0

介面操作介紹



Create Virtual Machine

CDX of IE8 on Win7

...

system

Se

Secur
dis
de
secur
log
base
contains Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA, Xplico, NetworkMiner, and

and includes exclusive custom-made tools created by AppSec Labs.

system

CDX of owasp-bwa-V1

OWASP Broken Web Applications Project is a collection of vulnerable web applications that is distributed on a Virtual Machine. username:root

system

介面操作練習時間

- 網頁：cdx.nchc.org.tw
- VPN 連線
  - remote gateway:140.110.112.1
- 第一步 VPN 連線
  - 方式1:登入 CDX 網頁再登入 CDX 平台
  - 方式2:直接登入CDX 平台
    - http://192.168.66.160:9869/

CDX 攻防平台實務

- VM 部署流程
- VM 如何取得終端機
- VM 如何取得 IP
- VM 登入方式的選擇
  - 帳號密碼設定
  - 公鑰私鑰認證
- VM 開機如何重設每一台主機密碼

CDX 攻防平台實務

- VM 部署流程
  - 映像檔
  - cpu + memory + network
    - 硬體相關 KVM 參數
  - VM 內的其它資訊
    - 製造 cdrom 映像檔帶入VM內
  - 拷備差異的部分-教室大量部署
  - 完整拷備-要實作自己的映像檔案

CDX 攻防平台實務

- VM 如何取得終端機?
  - KVM提供
  - frontend 透過 vnc-proxy 接到每台 KVM中的VM
-

CDX 攻防平台實務

- VM 如何取得 IP？
-

CDX 攻防平台實務

- VM 登入方式的選擇
  - 帳號密碼設定
  - 公鑰私鑰認證
- VM 開機如何重設每一台主機密碼
  - AD
  - LDAP

系統安全

系統安全

- 網路連接讓許多的電腦彼此之間可以互相的溝通，透過一些通訊協定帶動了許多的應用服務。在享受便利的同時往往也產生了許多的安全性問題，因此不太可能建構出一個絕對安全的系統或是網路架構。
- 管理者一定要清楚知道網路中存在哪些威脅、哪些人需要特定的授權，並且從系統及架構中評估整體可能遭受的實體安全或是系統網路安全可能帶來的威脅，並且根據可能的狀況評估相對的防禦措施。

常見的網路威脅

- 常見的網路威脅
  - 病毒和惡意程式
  - 間諜程式和可能的資安威脅程式
  - 垃圾郵件
  - 入侵
  - 惡意行為
  - 偽冒的存取點

常見的網路威脅

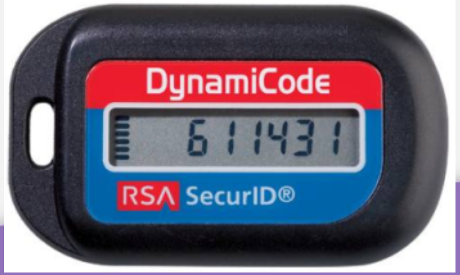
- 網路釣魚事件
- 大量郵件攻擊
- 網路安全威脅
- 無法清除病毒的檔案

威脅 and 弱點

Which came first, the chicken or the egg

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

SQL injection T Shirts

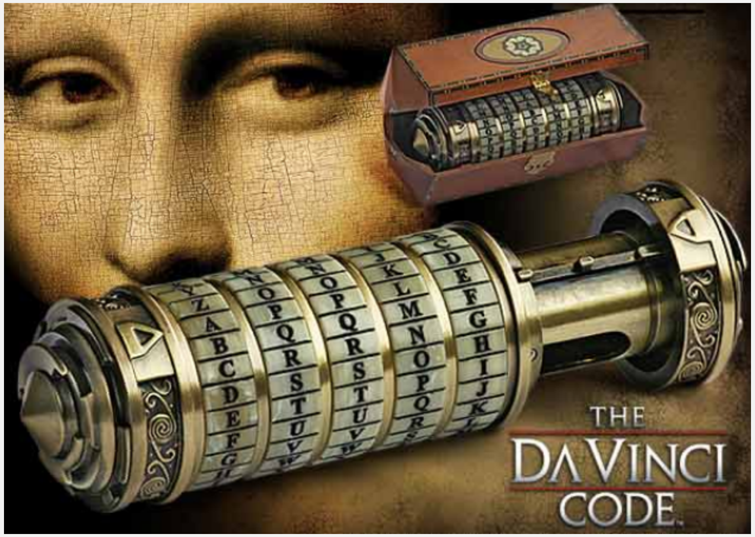
' OR 1=1--
SELECT * FROM USERS WHERE ID='ADMIN' AND PASSWORD='' OR '1'='1'

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

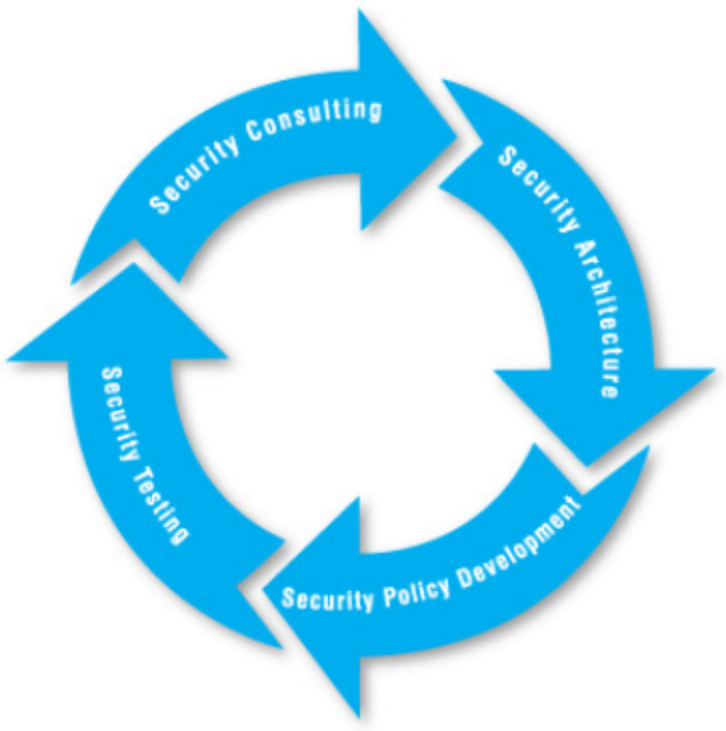
- Operations Security 操作安全
  - 資訊系統之防護與管理
  - 系統異動管理
  - 特權個體之控管

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

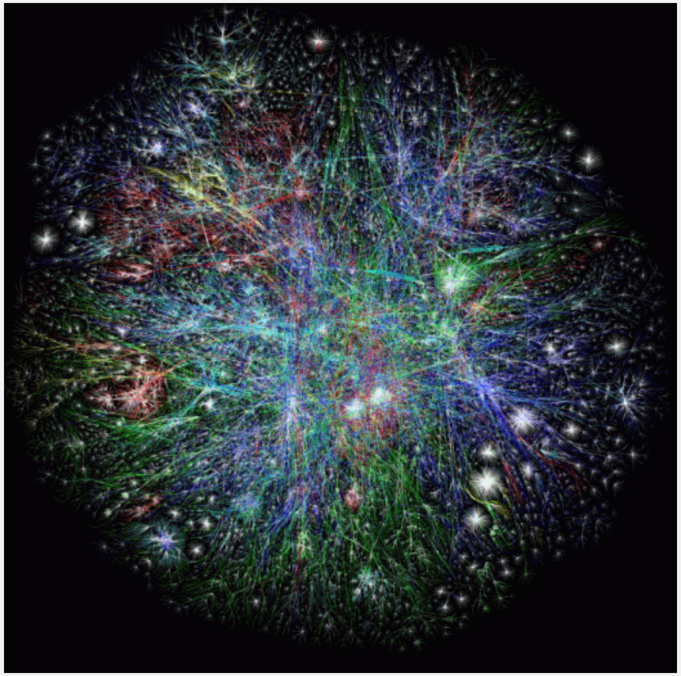
資訊安全十大領域

- 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



Security ?

Government Configuration Baseline

- 政府組態基準(Government Configuration Baseline，簡稱GCB)目的在於規範資通訊終端設備的一致性安全設定，以降低成為駭客入侵管道，進而引發資安事件之疑慮。
  - https://www.nccst.nat.gov.tw/GCB?lang=zh
  - https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline/faqs

Hardening Wiki

- In computing, hardening is usually the process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions; in principle a single-function system is more secure than a multipurpose one. Reducing available ways of attack typically includes changing default passwords, the removal of unnecessary software, unnecessary usernames or logins, and the disabling or removal of unnecessary services.

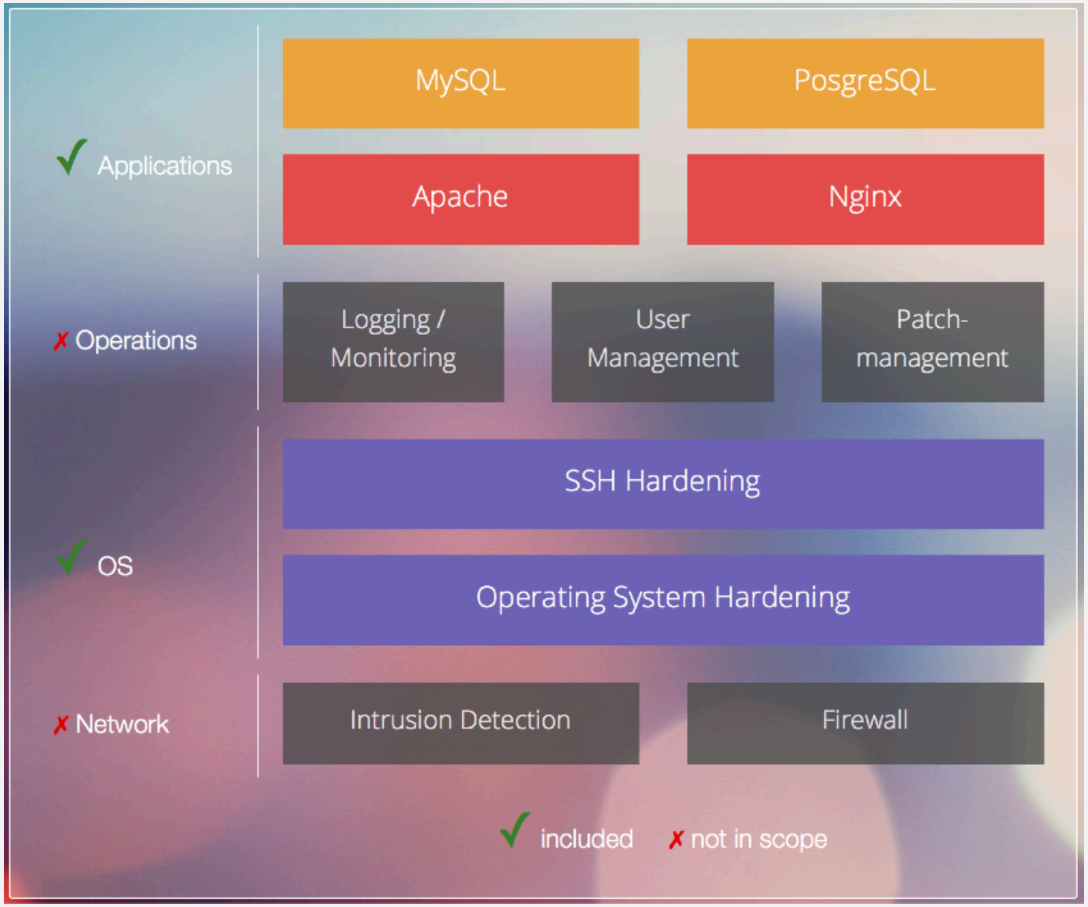
Hardening

- Hardening activities include:
  - Keeping security patches updated
  - Installing firewall
  - Closing certain ports
  - Not allowing file sharing among programs
  - Installing virus and spyware protection
  - Using containers or virtual machines

Hardening

- – Creating strong passwords
- – Keeping a backup
- – Disabling cookies
- – Using encryption when possible
- – Disabling weak encryption

Hardening Framework



✓ Applications
- MySQL
- PosgreSQL
- Apache
- Nginx

✗ Operations
- Logging / Monitoring
- User Management
- Patch-management

✓ OS
- SSH Hardening
- Operating System Hardening

✗ Network
- Intrusion Detection
- Firewall

✓ included ✗ not in scope

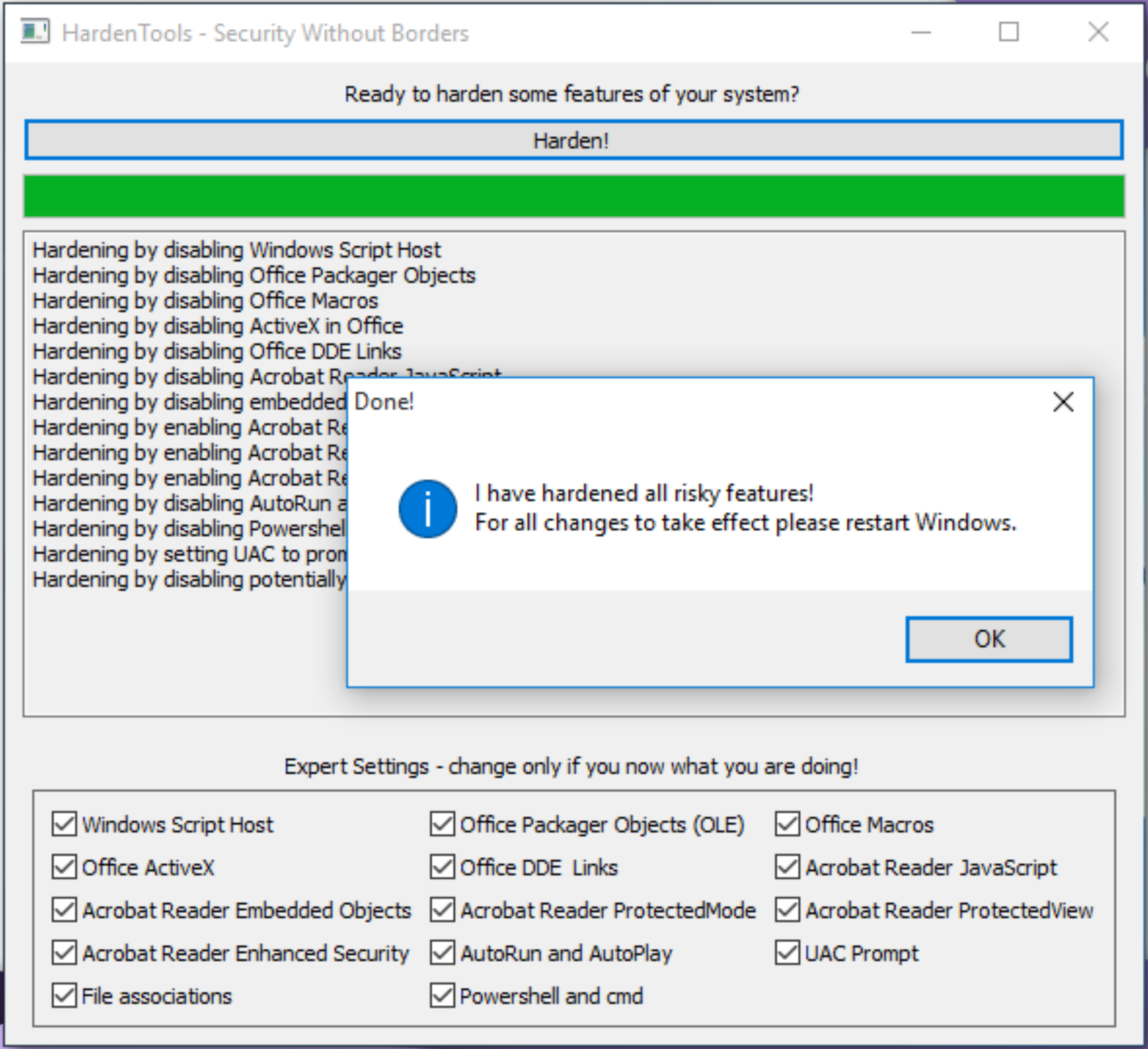
https://dev-sec.io/

Hardentools

- Hardentools is a collection of simple utilities designed to disable a number of "features" exposed by operating systems , and primary consumer applications. These features, commonly thought for Enterprise customers, are generally useless to regular users and rather pose as dangers as they are very commonly abused by attackers to execute malicious code on a victim's computer.

Hardentools

- The intent of this tool is to simply reduce the attack surface by disabling the low-hanging fruit. Hardentools is intended for individuals at risk, who might want an extra level of security at the price of some usability. It is not intended for corporate environments.
- https://github.com/securitywithoutborders/hardentools



Ready to harden some features of your system?

```
Hardening by disabling Windows Script Host
Hardening by disabling Office Packager Objects
Hardening by disabling Office Macros
Hardening by disabling ActiveX in Office
Hardening by disabling Office DDE Links
Hardening by disabling Acrobat Reader JavaScript
Hardening by disabling embedded
Hardening by enabling Acrobat Re
Hardening by enabling Acrobat Re
Hardening by enabling Acrobat Re
Hardening by disabling AutoRun a
Hardening by disabling Powershel
Hardening by setting UAC to prom
Hardening by disabling potentially
```

Done!

I have hardened all risky features!
For all changes to take effect please restart Windows.

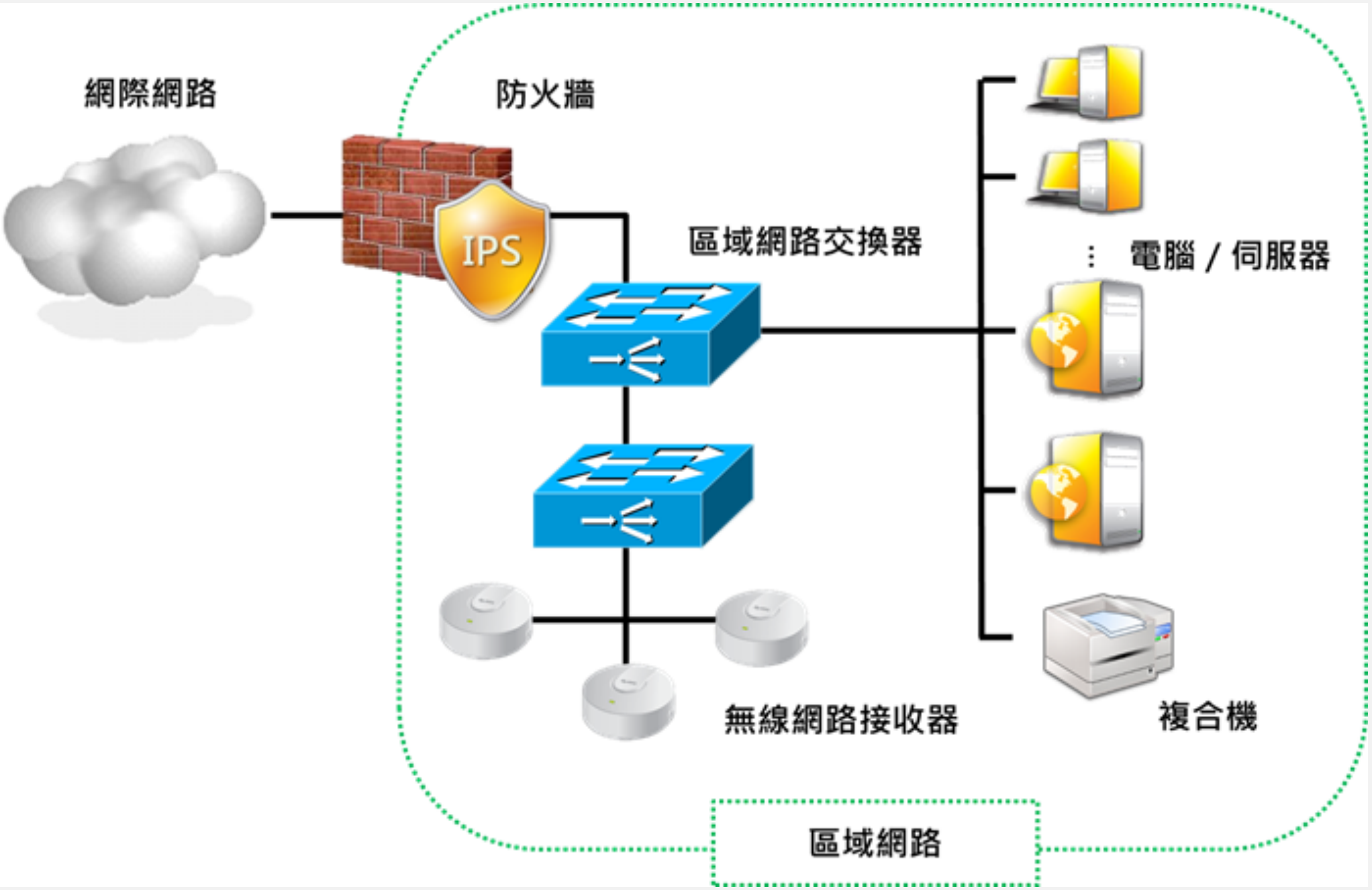
Expert Settings - change only if you now what you are doing!

☑ Windows Script Host ☑ Office Packager Objects (OLE) ☑ Office Macros
☑ Office ActiveX ☑ Office DDE Links ☑ Acrobat Reader JavaScript
☑ Acrobat Reader Embedded Objects ☑ Acrobat Reader ProtectedMode ☑ Acrobat Reader ProtectedView
☑ Acrobat Reader Enhanced Security ☑ AutoRun and AutoPlay ☑ UAC Prompt
☑ File associations ☑ Powershell and cmd

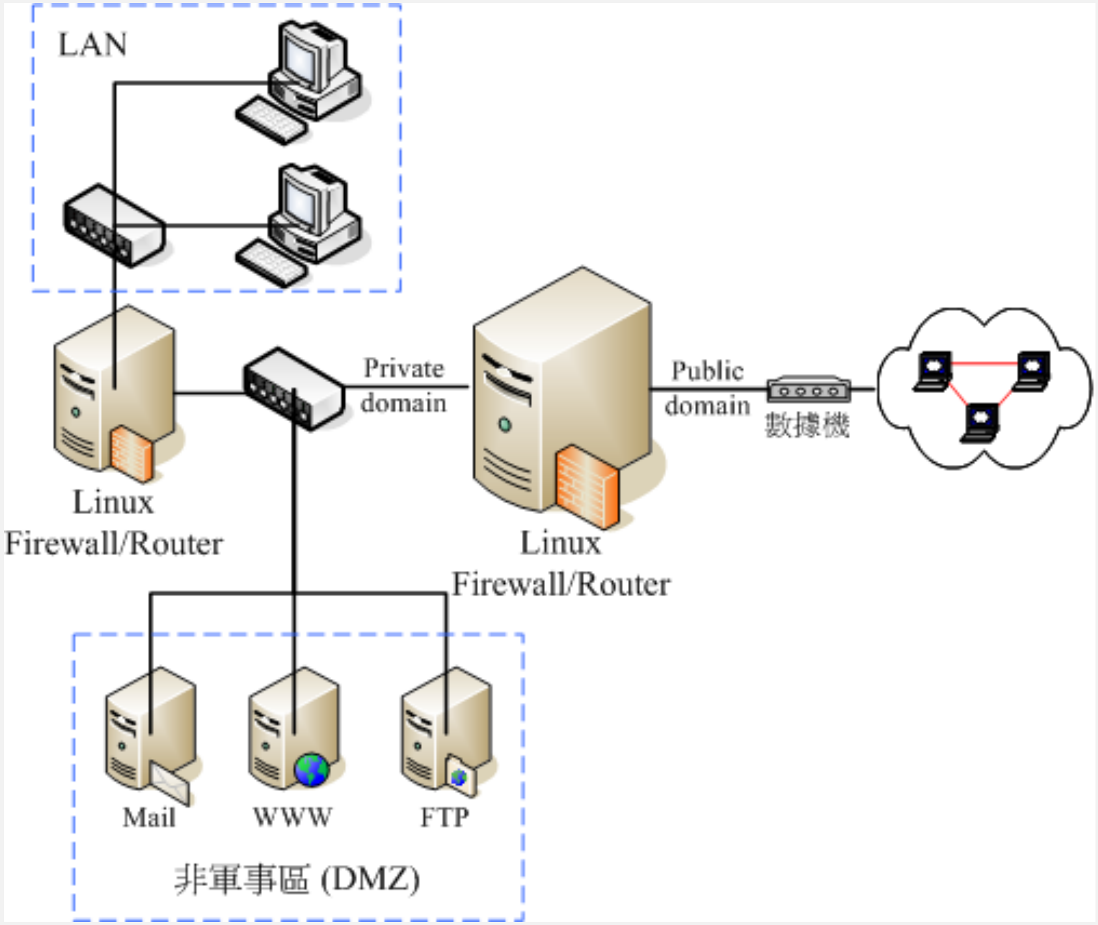
系統網路安全架構探討

- 目前許多常見的系統及應用服務都會透過多種不同的軟硬體組合而成，主要是透過網路設備、資安設備、系統主機等等硬體以及軟體構成一個系統網路架構。
- 在這個架構下需要思考如何提升安全性，透過人員、相關服務、政策等等擬定安全架構，例如防火牆部分採用黑名單或是白名單、系統及系統之間來源是否做限制、系統人員授權之權限，以及是否有符合一些國際資安標準，如 ISO 27001 、CSA STAR 等等。

常見的系統網路架構



常見的系統網路架構


LAN
Private domain
Public domain
數據機
Linux Firewall/Router
Linux Firewall/Router
Mail
WWW
FTP
非軍事區 (DMZ)

思考題

- 請問上述的架構上，你如何做好安全規劃呢？

系統與應用程式弱點檢測

系統及應用程式檢測

- 系統及應用程式為什麼需要檢測呢？
  - 了解運作過程中可能會產生的問題
  - 減少系統除錯時間
  - 了解系統及應用程式上限承載能力
  - 降低後續維運的成本
  - 減少資訊安全所帶來的問題

系統及應用程式安全檢測

- 系統及應用程式安全檢測是透過一些資訊安全工具，進行安全性測試，常見的測試包含了以下：
  - 壓力測試
  - 網路服務測試
  - 應用程式參數測試
  - 服務弱點探測
  - 系統弱點探測
  - 密碼測試
  - ….

弱點掃描

- 正所謂「水可載舟，亦可覆舟」，對於資安人員來說，善用弱點掃描的技術可以幫助他們了解所管理的設備是否存在漏洞，進而修補漏洞並將漏洞所造成的風險降到最低。對於駭客而言弱點掃描，是一種得力的攻擊工具，攻擊者一旦取得了目標主機或設備的相關漏洞，後續便可以利用這些漏洞針對目標進行攻擊行為。

弱點掃描的定義

- 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

弱點掃描的定義

- 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

常見的弱點掃描程式

- Lynis
- Nessus
- Nxpose
- Vulns
- OpenVAS

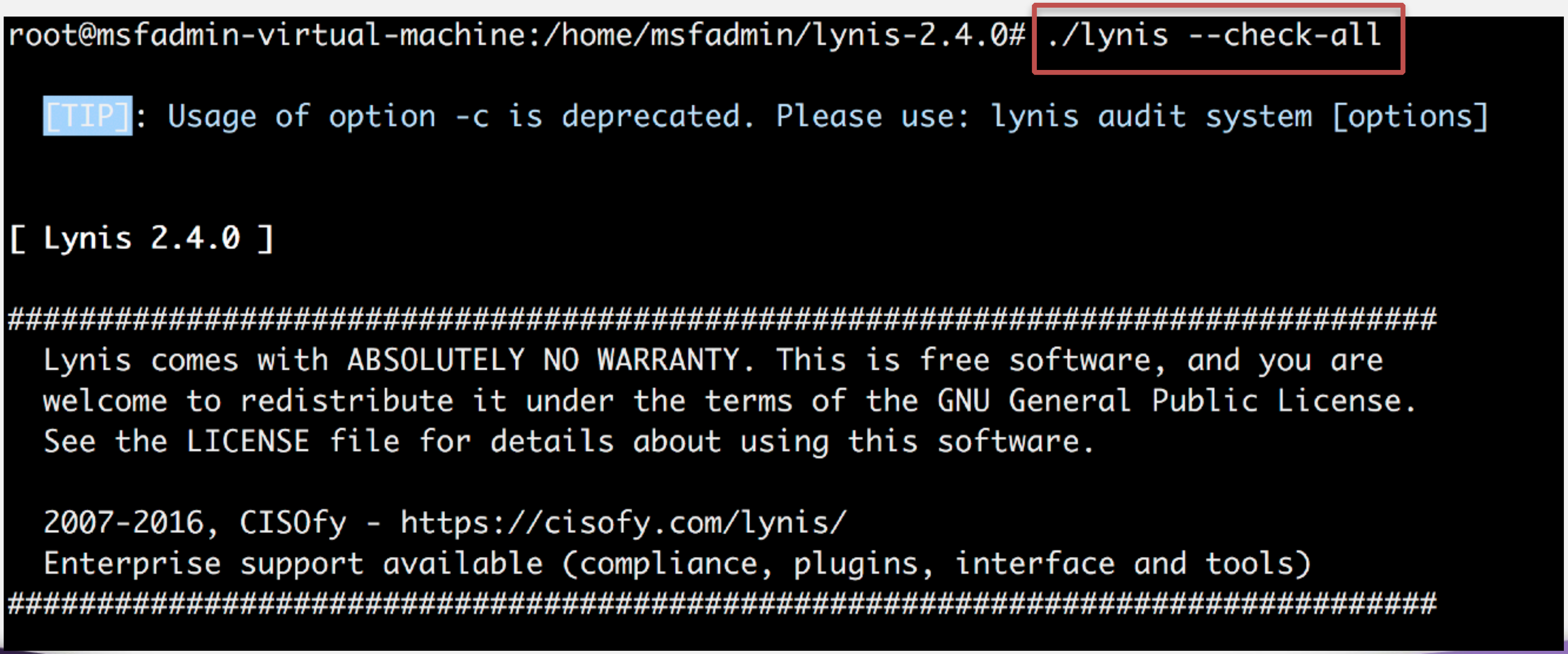
Lynis

- Lynis is a security auditing tool for systems running Linux, macOS, or Unix. It can be used for security assessments and configuration audits.
- https://cisofy.com/lynis/

CISOFY
AUDITING-HARDENING-COMPLIANCE

Lynis

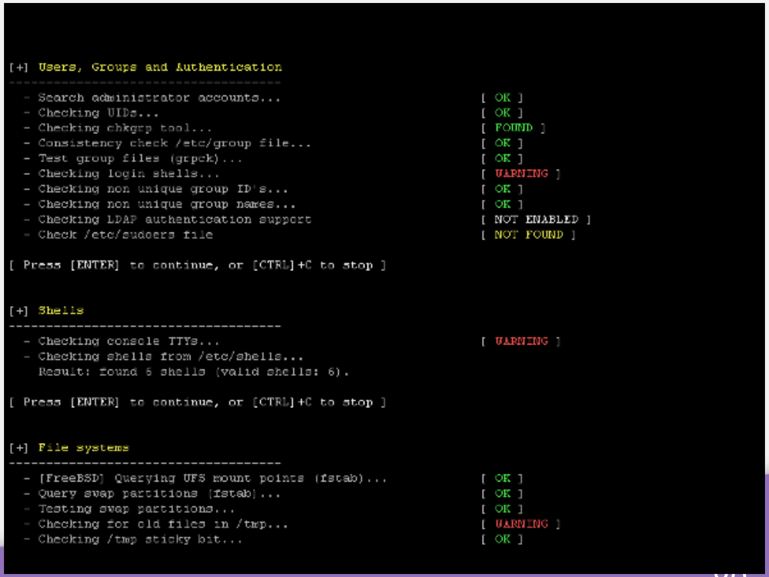
- 開啟終端機
  - ./lynis —check-all



```
root@msfadmin-virtual-machine:/home/msfadmin/lynis-2.4.0# ./lynis --check-all

  [TIP]: Usage of option -c is deprecated. Please use: lynis audit system [options]


[ Lynis 2.4.0 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2016, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################
```

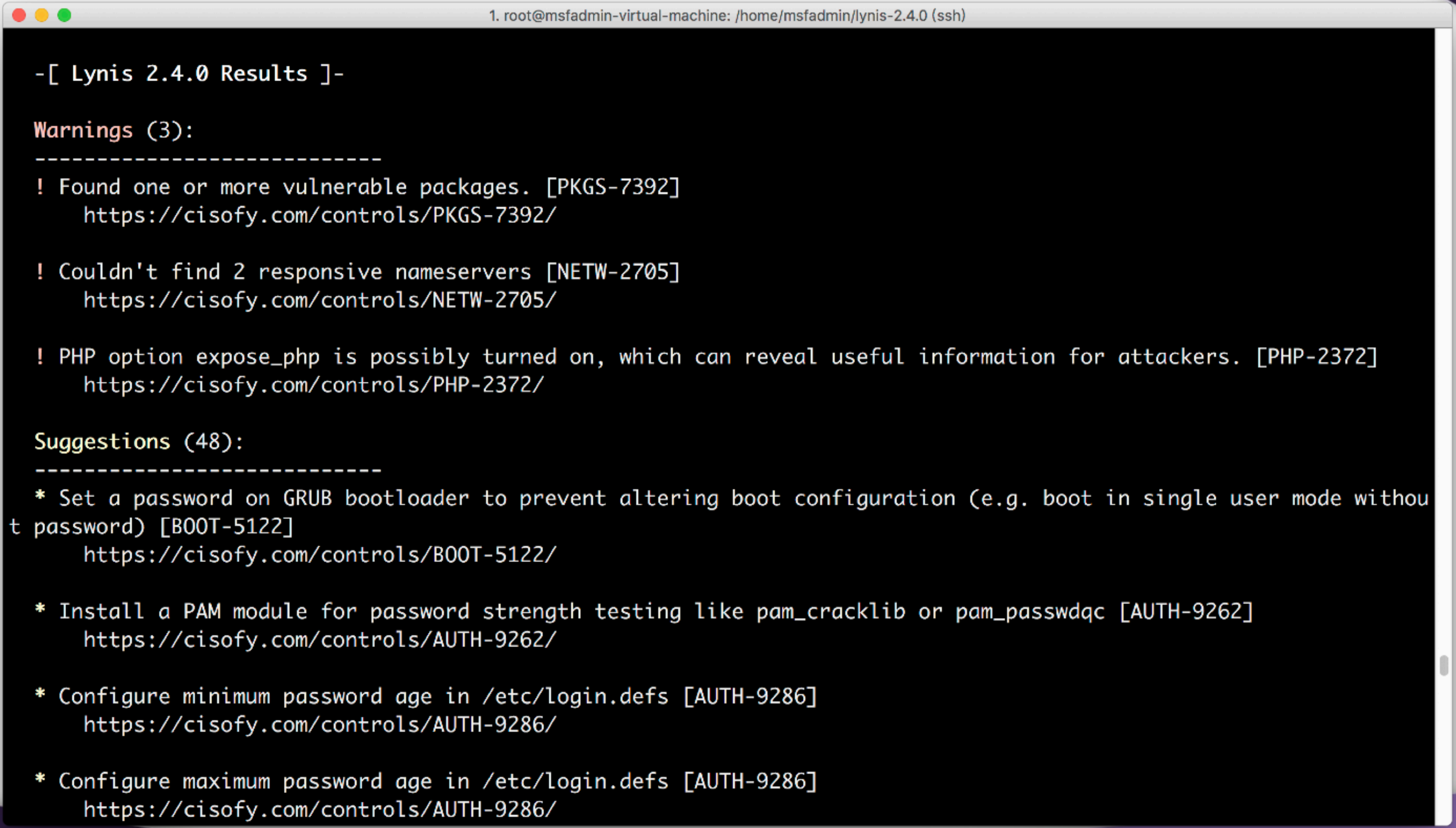
Lynis

- wget https://downloads.cisofy.com/lynis/lynis-2.6.6.tar.gz
- tar -zxvf lynis-2.6.6.tar.gz
- sudo chown -R 0:0 lynis
- cd lynis/
- ./lynis audit system



```
[+] Users, Groups and Authentication
------------------------------------
  - Search administrator accounts...                          [ OK ]
  - Checking UIDs...                                          [ OK ]
  - Checking chkgrp tool...                                   [ FOUND ]
  - Consistency check /etc/group file...                      [ OK ]
  - Test group files (grpck)...                               [ OK ]
  - Checking login shells...                                  [ WARNING ]
  - Checking non unique group ID's...                         [ OK ]
  - Checking non unique group names...                        [ OK ]
  - Checking LDAP authentication support                      [ NOT ENABLED ]
  - Check /etc/sudoers file                                   [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]


[+] Shells
------------------------------------
  - Checking console TTYs...                                  [ WARNING ]
  - Checking shells from /etc/shells...
    Result: found 6 shells (valid shells: 6).

[ Press [ENTER] to continue, or [CTRL]+C to stop ]


[+] File systems
------------------------------------
  - [FreeBSD] Querying UFS mount points (fstab)...            [ OK ]
  - Query swap partitions (fstab)...                          [ OK ]
  - Testing swap partitions...                                [ OK ]
  - Checking for old files in /tmp...                         [ WARNING ]
  - Checking /tmp sticky bit...                               [ OK ]
```

Results



1. root@msfadmin-virtual-machine: /home/msfadmin/lynis-2.4.0 (ssh)

```
  -[ Lynis 2.4.0 Results ]-

  Warnings (3):
  ----------------------------
  ! Found one or more vulnerable packages. [PKGS-7392]
      https://cisofy.com/controls/PKGS-7392/

  ! Couldn't find 2 responsive nameservers [NETW-2705]
      https://cisofy.com/controls/NETW-2705/

  ! PHP option expose_php is possibly turned on, which can reveal useful information for attackers. [PHP-2372]
      https://cisofy.com/controls/PHP-2372/

  Suggestions (48):
  ----------------------------
  * Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in single user mode withou
t password) [BOOT-5122]
      https://cisofy.com/controls/BOOT-5122/

  * Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
      https://cisofy.com/controls/AUTH-9262/

  * Configure minimum password age in /etc/login.defs [AUTH-9286]
      https://cisofy.com/controls/AUTH-9286/

  * Configure maximum password age in /etc/login.defs [AUTH-9286]
      https://cisofy.com/controls/AUTH-9286/
```

Nessus

- Nessus is a proprietary vulnerability scanner developed by Tenable Network Security. It is free of charge for personal use in a non-enterprise environment.
- According to surveys done in 2009 by sectools.org, Nessus is the world's most popular vulnerability scanner, taking first place in the 2000, 2003, and 2006 security tools survey. Tenable Network Security estimated in 2005 that it was used by over 75,000 organizations worldwide.

Nexpose

- Rapid7 Nexpose is a vulnerability scanner which aims to support the entire vulnerability management lifecycle, including discovery, detection, verification, risk classification, impact analysis, reporting and mitigation. It integrates with Rapid7's Metasploit for vulnerability exploitation. It is sold as standalone software, an appliance, virtual machine, or as a managed service or private cloud deployment. User interaction is through a web browser.

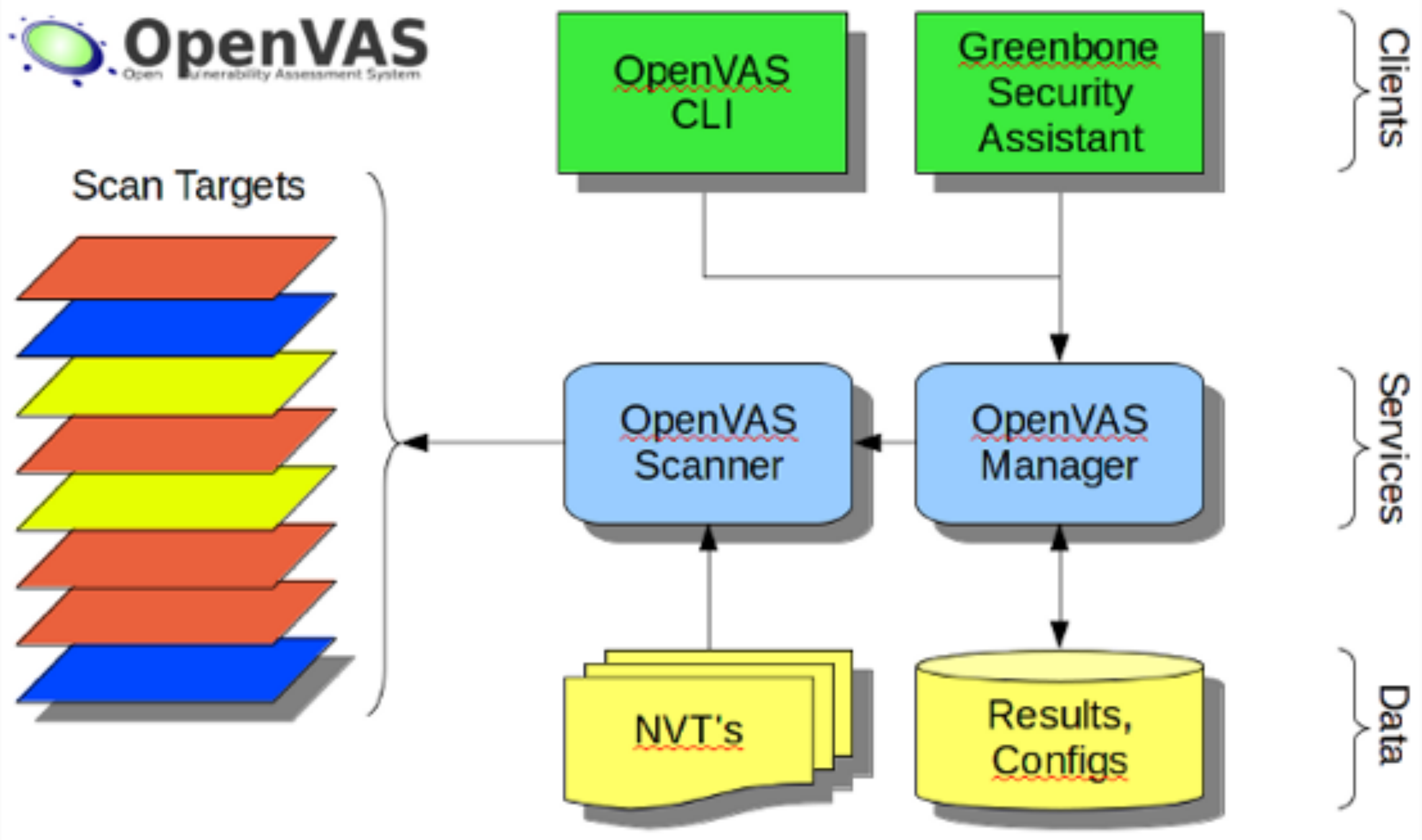
Vuls: VULnerability Scanner

- Vuls is a tool created to solve the problems listed above. It has the following characteristics.
  - Informs users of the vulnerabilities that are related to the system.
  - Informs users of the servers that are affected.
  - Vulnerability detection is done automatically to prevent any oversight.
  - Report is generated on regular basis using CRON or other methods to manage vulnerability.

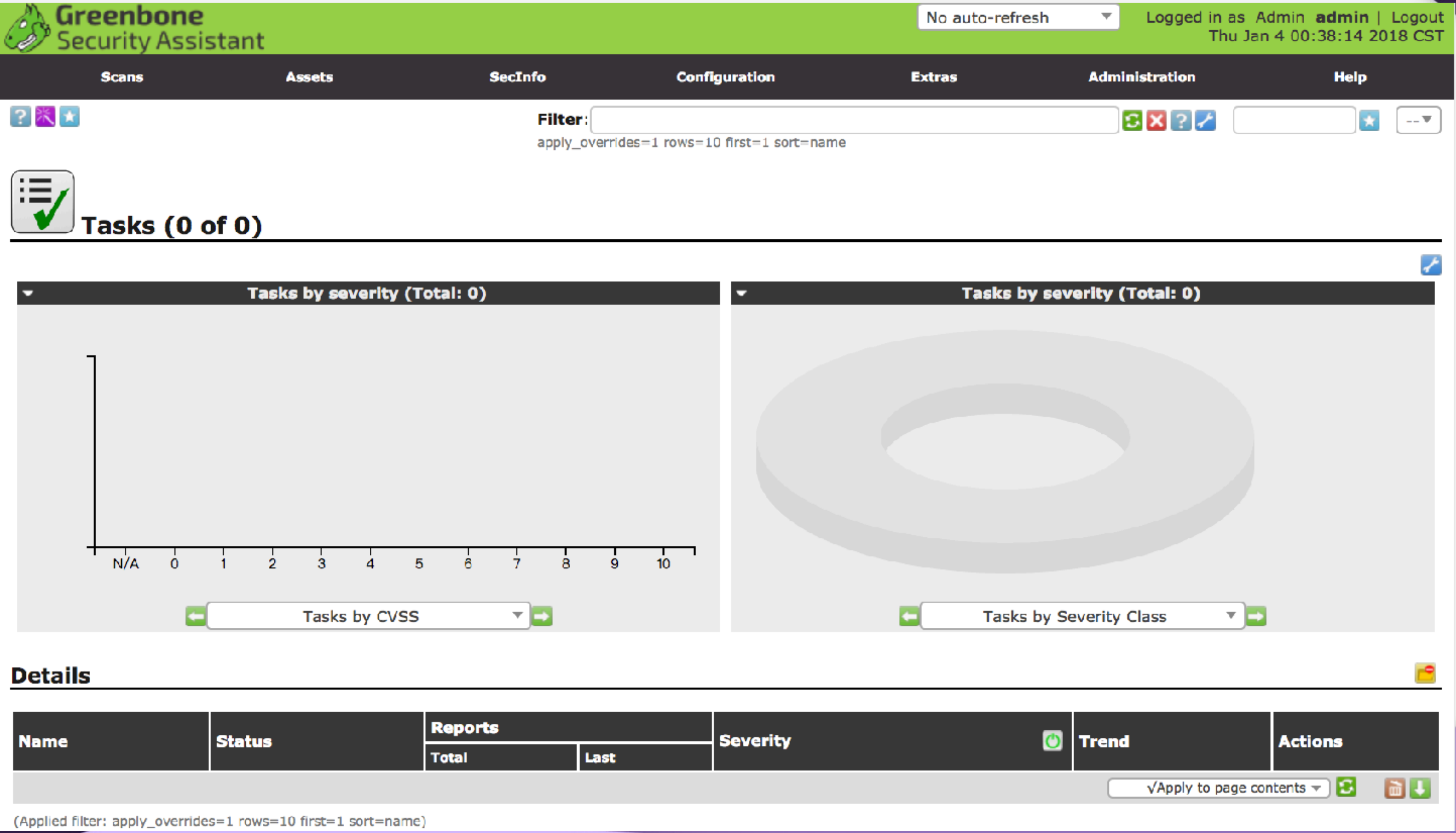
OpenVAS

- OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. The framework is part of Greenbone Networks' commercial vulnerability management solution from which developments are contributed to the Open Source community since 2009.

OpenVAS 架構


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

Greenbone



Logged in as Admin **admin** | Logout
Thu Jan 4 00:38:14 2018 CST

apply_overrides=1 rows=10 first=1 sort=name

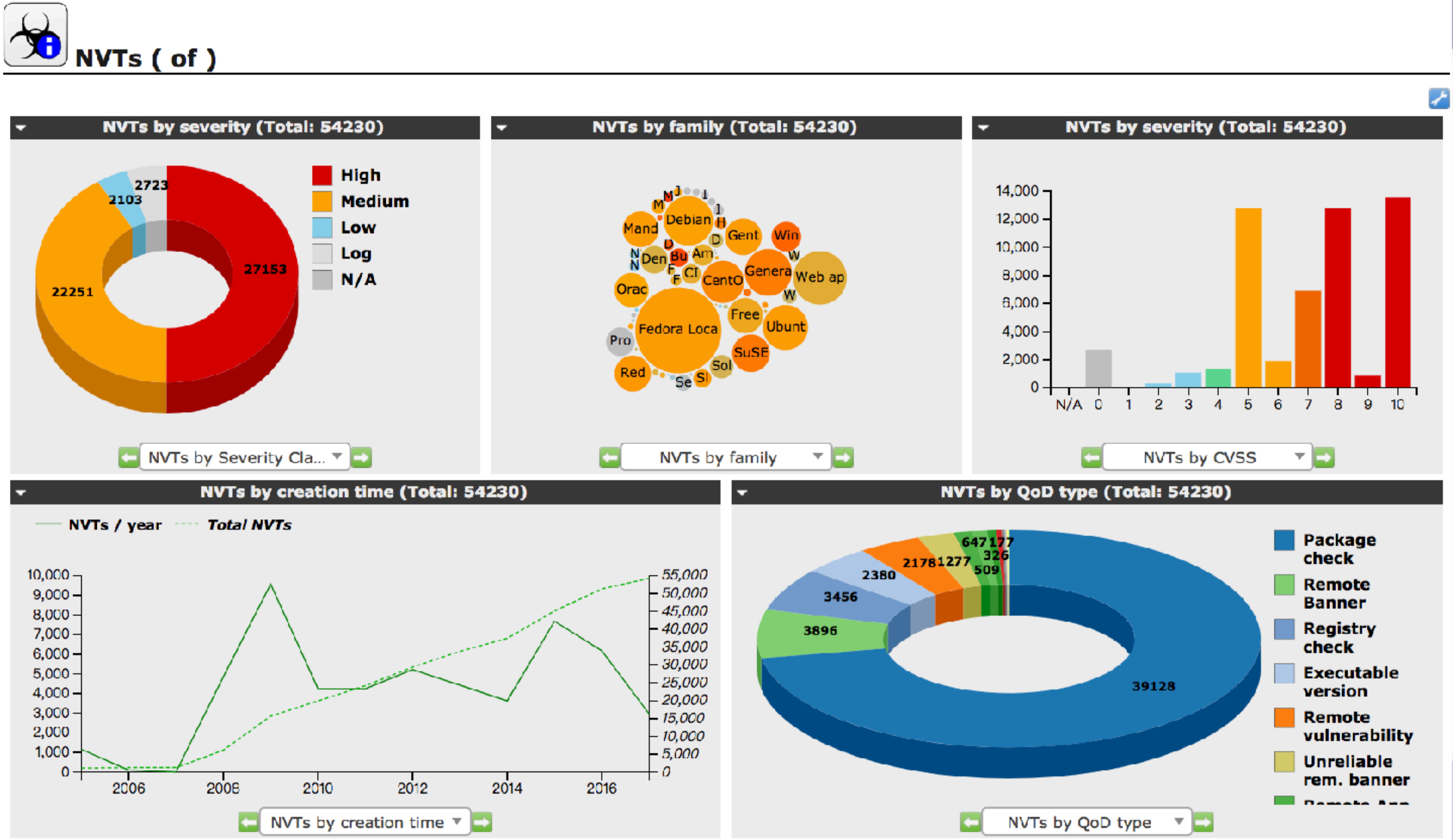
Tasks (0 of 0)

Details

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			

(Applied filter: apply_overrides=1 rows=10 first=1 sort=name)

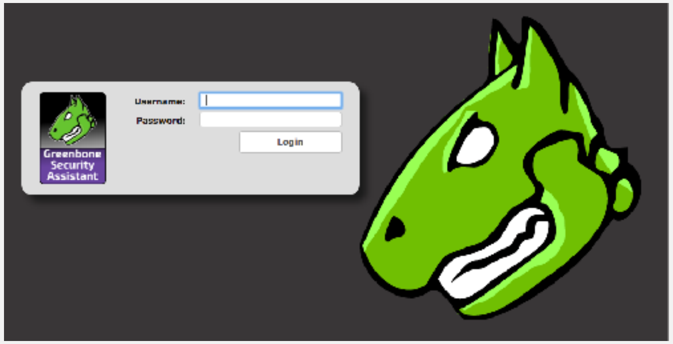
Greenbone



NVTs (of)

弱點掃描實作

- 請先開啟OpenVAS 環境，並且根據系統指定之IP ，利用Nmap 進行掃描，並且根據結果，來確認OpenVAS 服務是否正常啟動
- 開啟瀏覽器輸入IP 及Port
  - 帳號/密碼：admin/admin
- 請根據指定之IP進行弱點分析



思考問題

- 弱點掃瞄是如何進行的？
- 如果要知道掃瞄的內容，有什麼方式可以取得資訊？
- 如何進行弱點有效性或是存在與否的判斷？

問題與討論