MINISTRY OF ICT Smart Thailand

EGA

e-Government Agency

Electronic Government Agency (Public Organization)

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

การตรวจสอบช่องโหว่

(Vulnerability Assessment)

กำหนดการ

(Agenda)

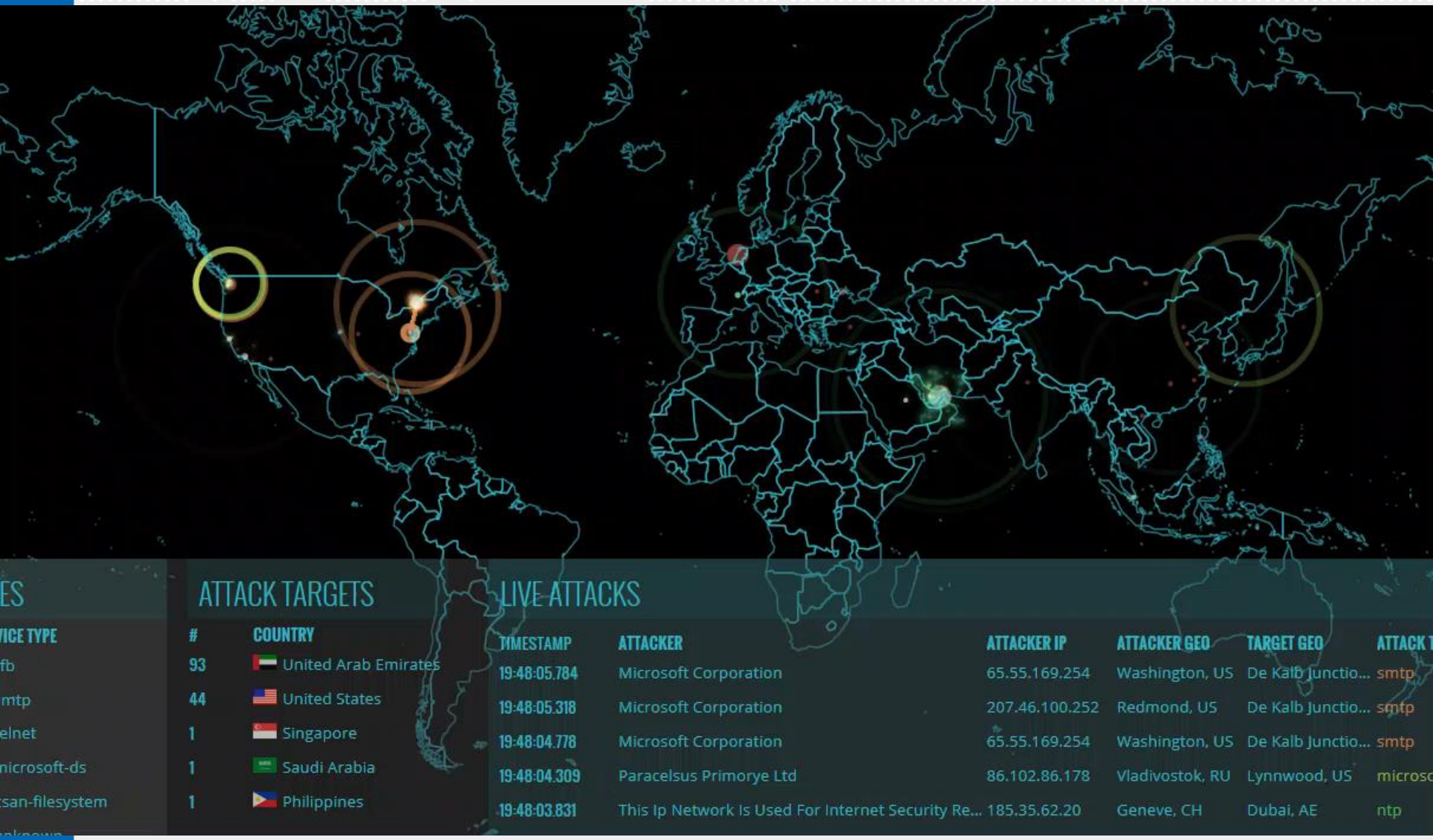
- Vulnerability Assessment ?
- การดำเนินการ **VA Scan**
- การดำเนินการหลังการ **VA Scan**

วัตถุประสงค์การตรวจสอบช่องโหว่

(Vulnerability Assessment Objectives)

- **Identifying (Services, ports, OS, IP, etc.)**
- **Quantifying**
- **Ranking**

ทำไมต้องตรวจสอบช่องโหว่



http://map.norsecorp.com

Identifying

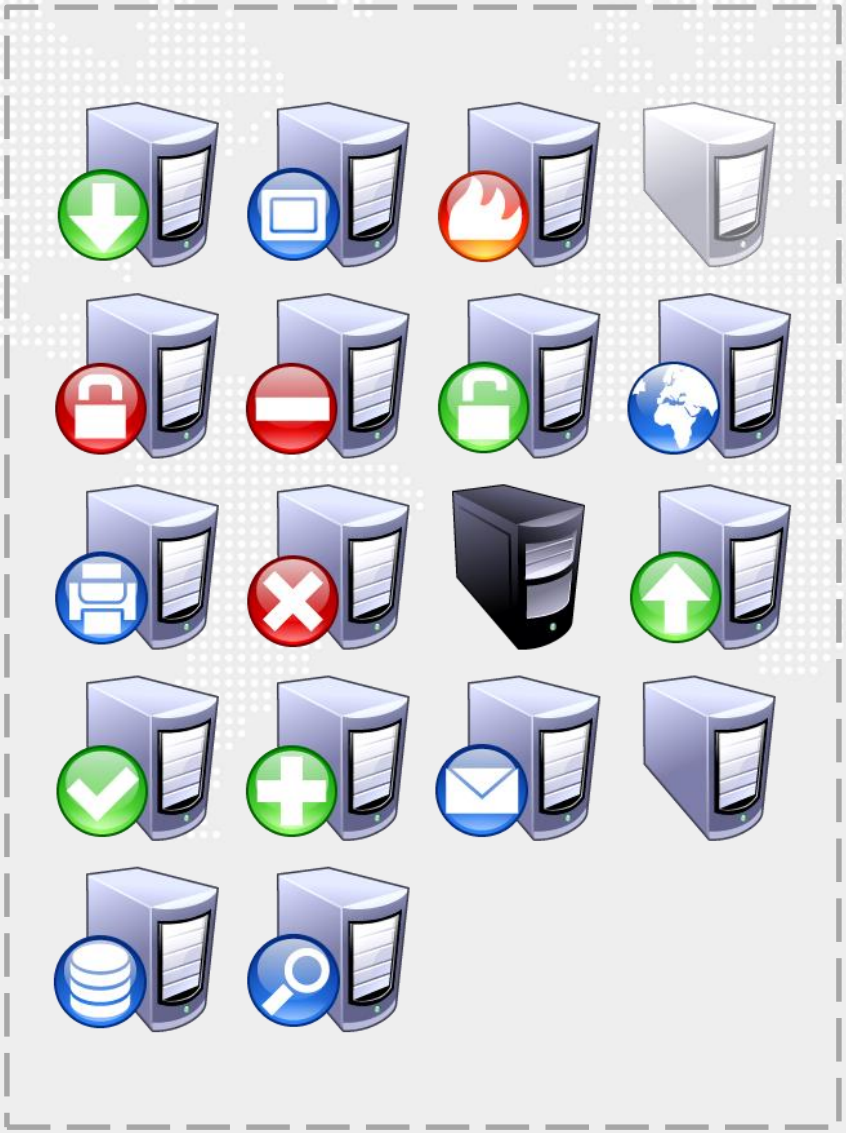
Web server
IP : 61.19.244.213
Port : 80,443

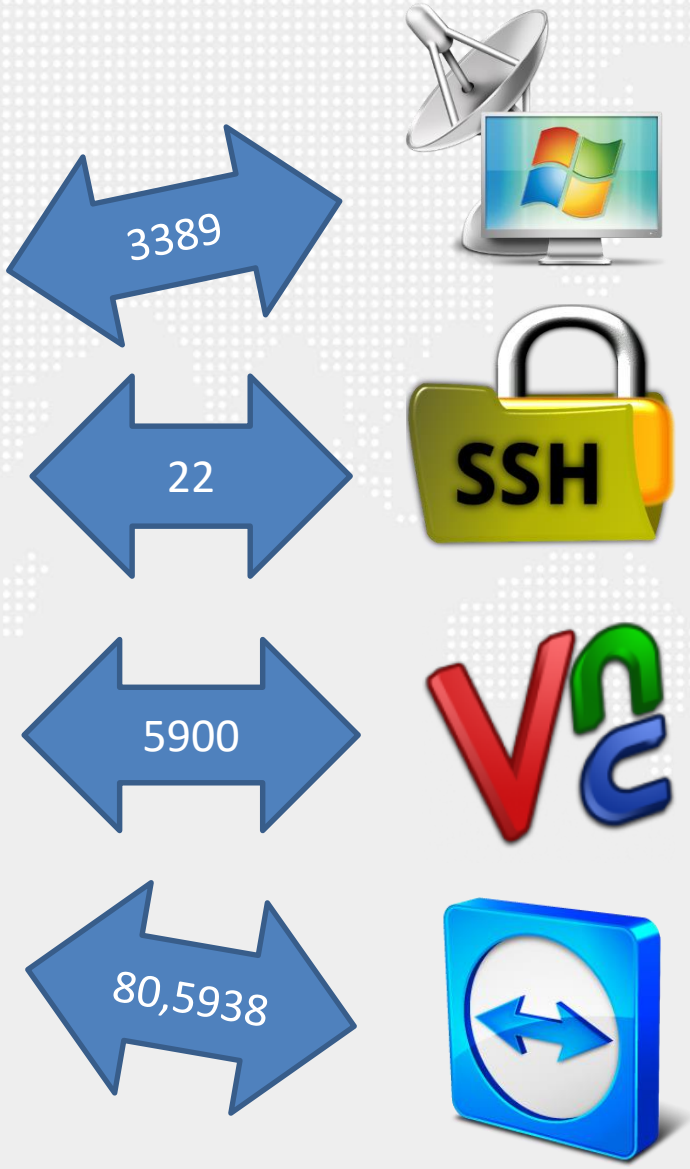
DNS server
IP : 61.19.244.215
Port : 53

Database server
IP : 61.19.244.214
Port : 3306,1433

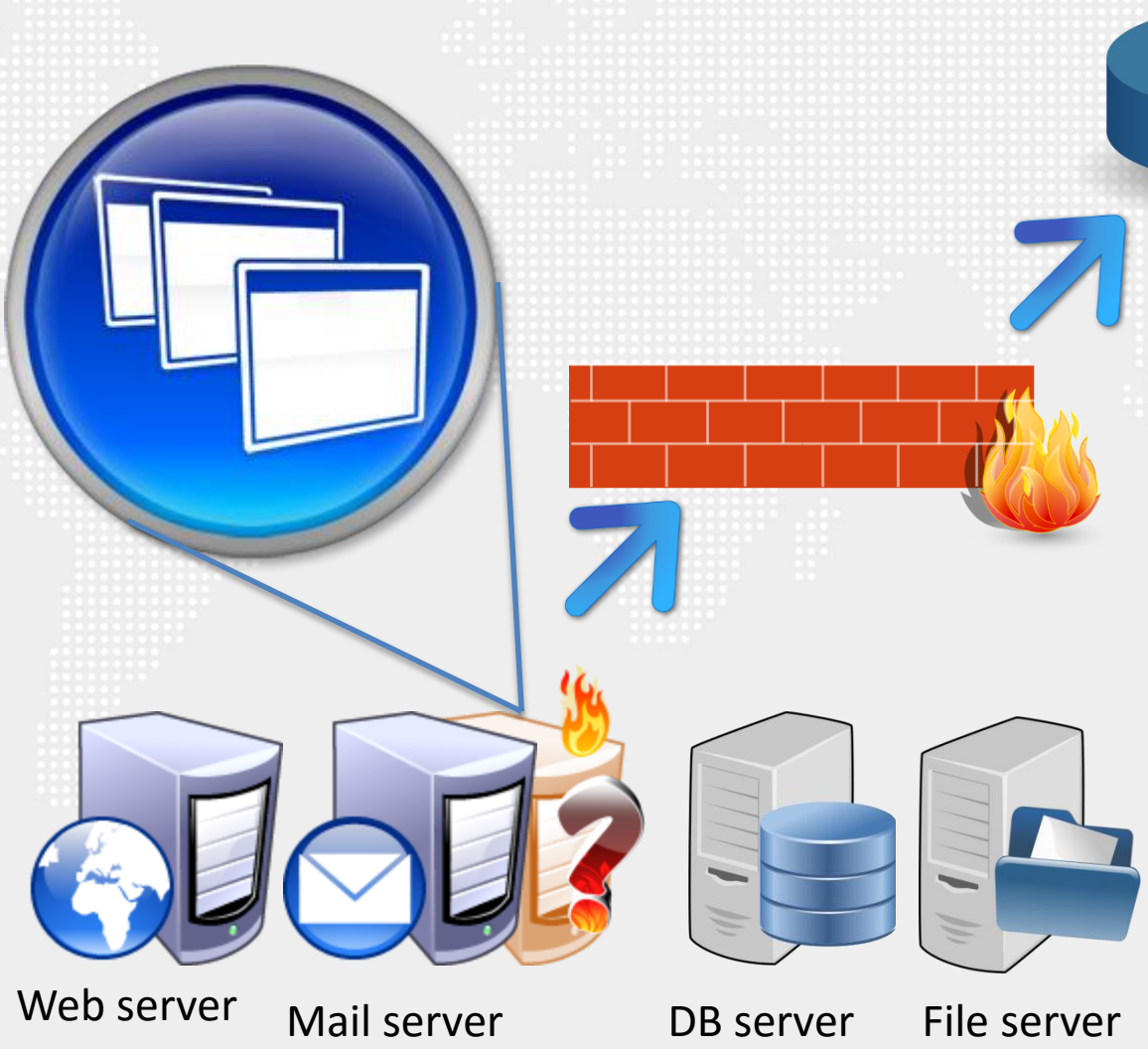
FTP server
IP : 61.19.244.216
Port : 21,22

Identifying

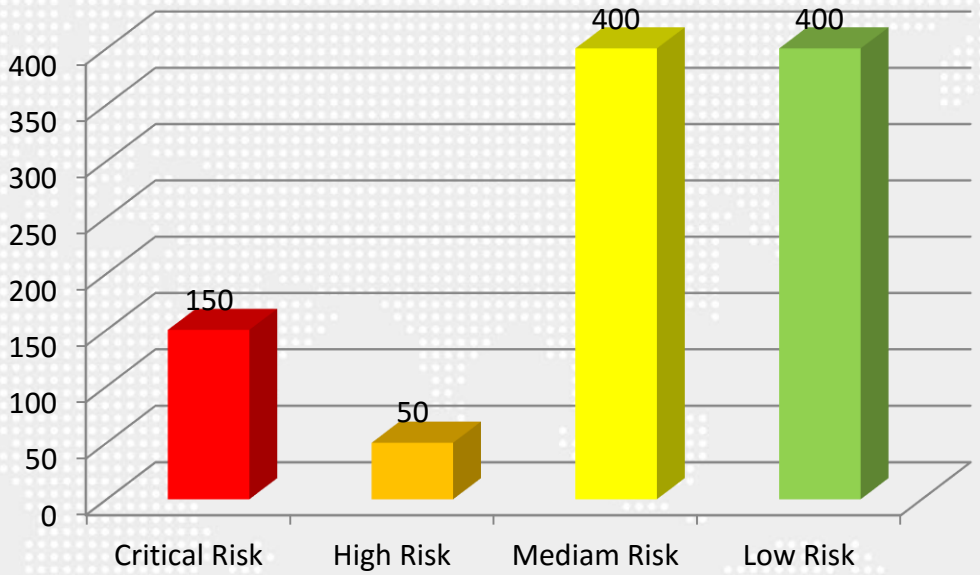


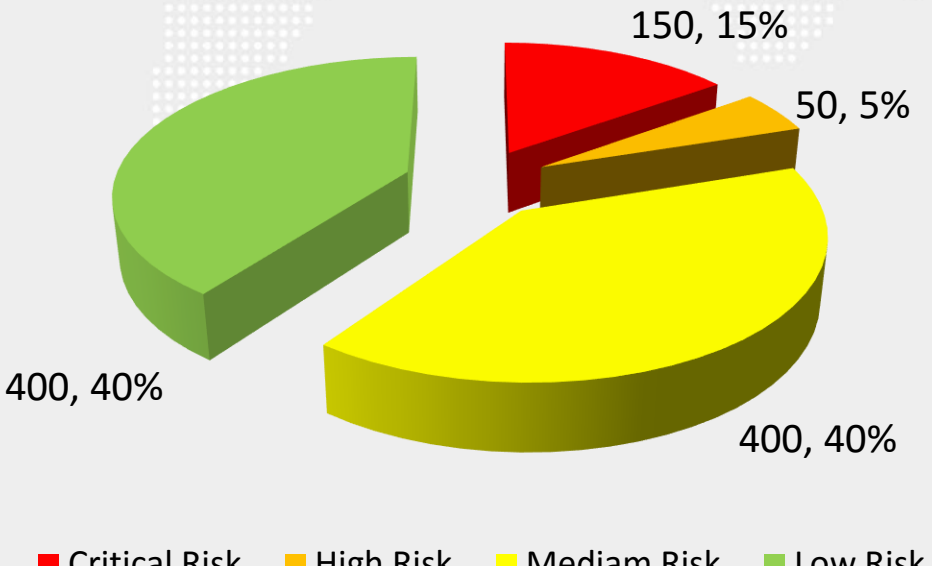


Identifying



Quantifying & Ranking





เป็นมาตรฐานสำหรับประเมินความรุนแรงของช่องโหว่ของระบบคอมพิวเตอร์ ซึ่งอยู่ภายใต้การดูแลของ NIST (National Institute of Standards and Technology) มีตัวชี้วัดเป็นจากการประเมินของผู้เชียวชาญเป็นช่วงคะแนนตั้งแต่ 0-10

Common Vulnerability Scoring System

เป็นมาตรฐานสำหรับประเมินความรุนแรงของช่องโหว่ของระบบคอมพิวเตอร์ ซึ่งอยู่ภายใต้การดูแลของ NIST (National Institute of Standards and Technology) มีตัวชี้วัดเป็นจากการประเมินของผู้เชียวชาญเป็นช่วงคะแนนตั้งแต่ 0-10

NIST	nexpose
High 7-10	critical 7.5-10
Medium 4-6.9	Severe 5-7.4
LOW 0-3.9	Moderate 3-4.9
	information < 2.9

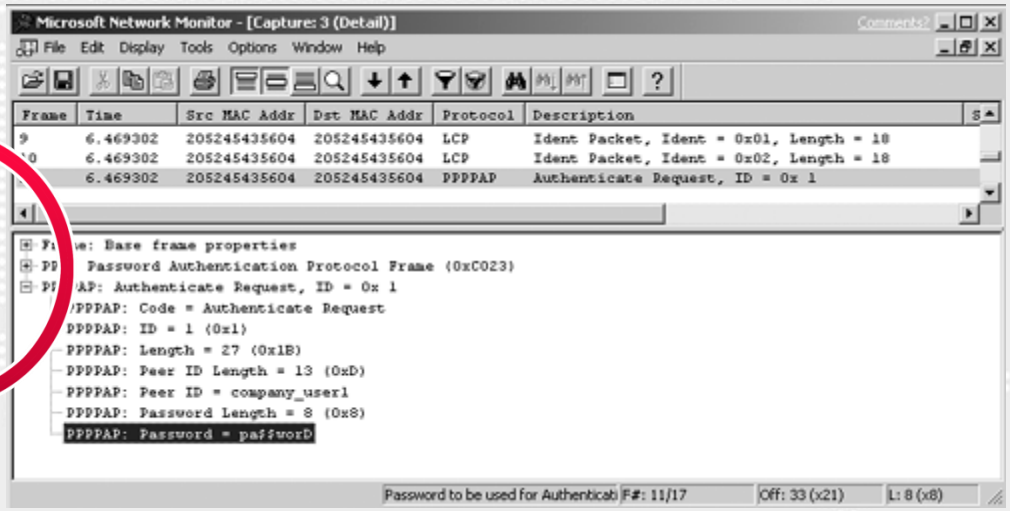
ระดับความเสี่ยง (Critical)

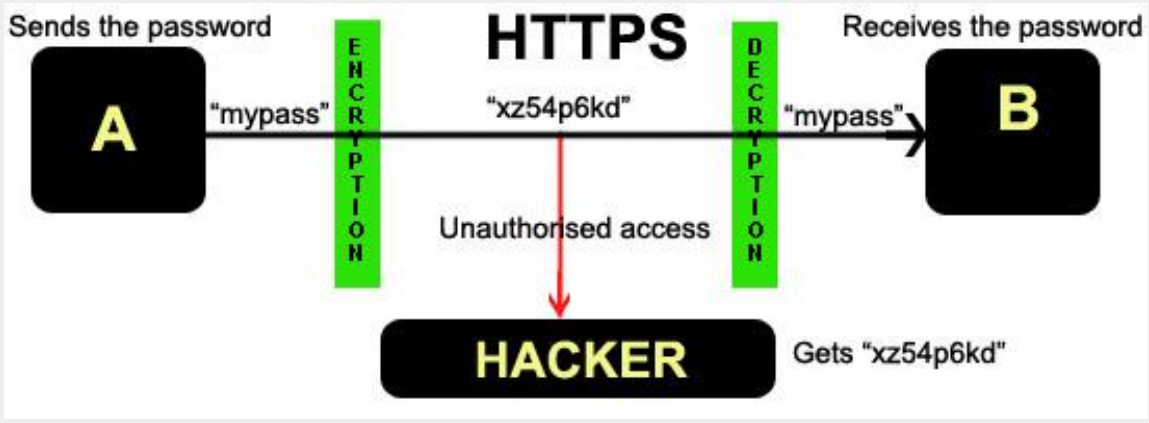
ความเสี่ยงระดับสูง (Critical) มีความเสี่ยงต่อการบุกรุกได้โดยง่าย ผู้บุกรุกสามารถใช้ช่องโหว่ที่ตรวจพบนี้โจมตีระบบและสามารถควบคุมระบบได้ทั้งหมด (Full Control) ควรจะต้องแก้ไขโดยเร่งด่วน

(CVSS Score 7.5-10)

ระดับความเสี่ยง (Severe)

ความเสี่ยงระดับรุนแรง(Severe) เป็นความเสี่ยงที่ผู้บุกรุกต้องใช้เวลามากขึ้นในการเจาะระบบ ไม่อาจเข้าถึงได้ทันทีแต่อาจเป็นองค์ประกอบที่ช่วยในการโจมตีสำเร็จ (CVSS Score 5 - 7.4)

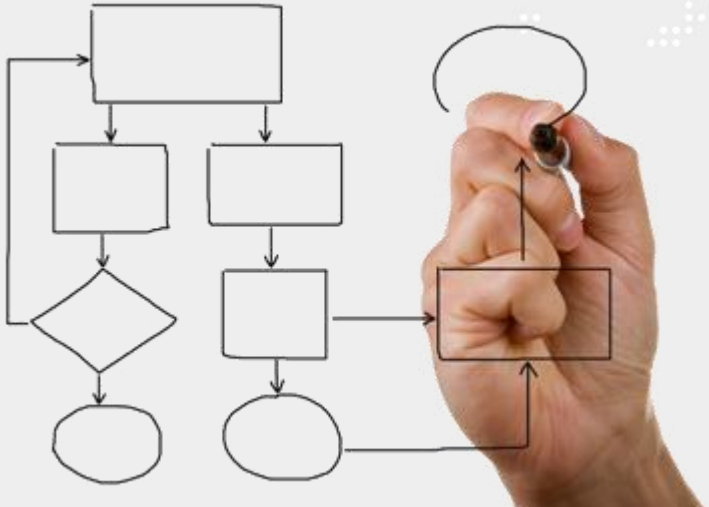




ระดับความเสี่ยง (Severe)

http://www.test.com/login.htm

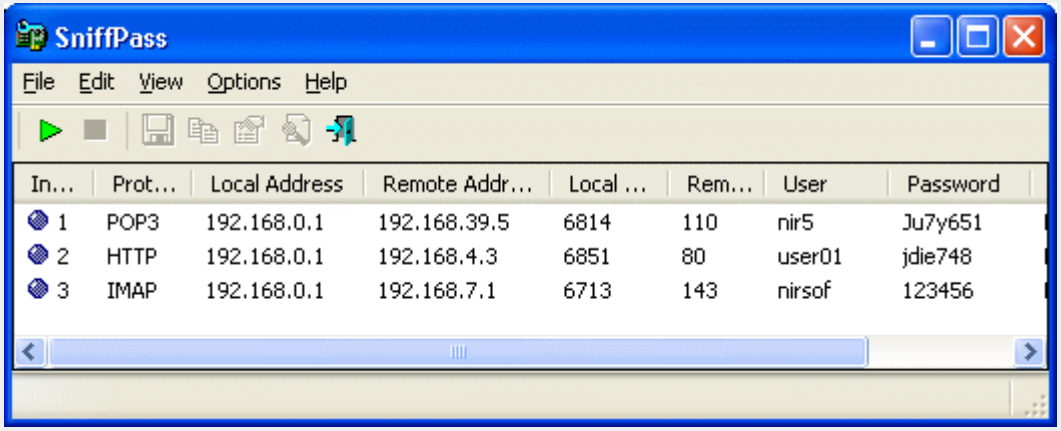
User_name = ‘Pongrapee’
Pass_word = ‘qwerty1234!@#$’



ระดับความเสี่ยง (Severe)

http://www.test.com/login.htm

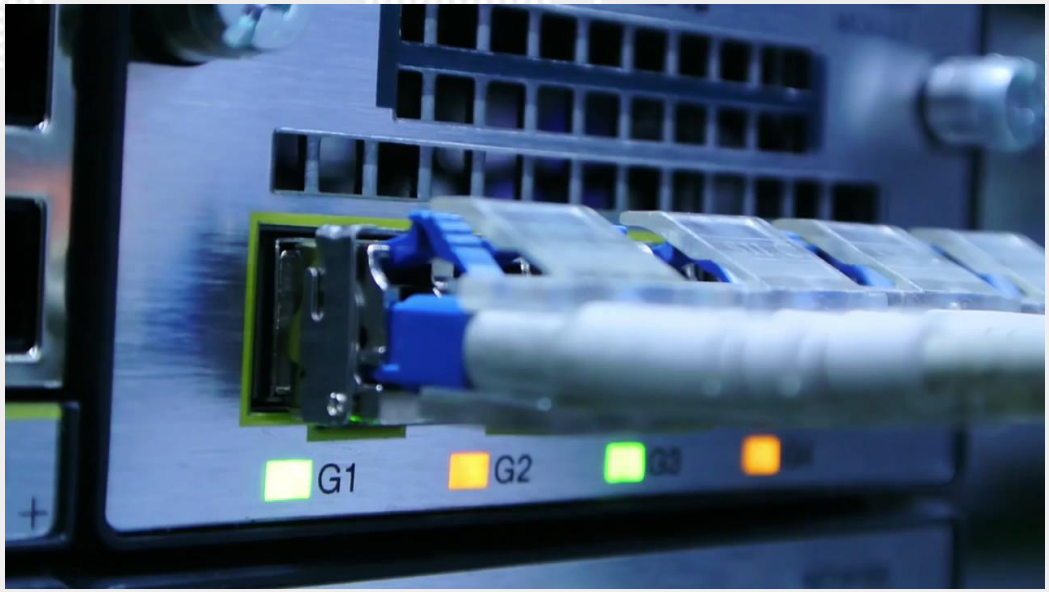
User_name = ‘Pongrapee’
Pass_word = ‘qwerty1234!@#$’



ระดับความเสี่ยง **(Moderate)**

ความเสี่ยงระดับปานกลาง (Moderate) เป็นช่องโหว่ที่ผู้บุกรุกไม่สามารถเจาะเข้าสู่ระบบได้โดยใช้ประโยชน์จากช่องโหว่ระดับปานกลางอย่างไรก็ตาม เพื่อความสมบูรณ์แบบของการสร้างความมั่นคงปลอดภัยให้แก่ระบบ เพราะช่องโหว่ดังกล่าวอาจพัฒนาเป็นช่องโหว่ที่มีความรุนแรงได้ในอนาคต

(CVSS Score 3 – 4.9)



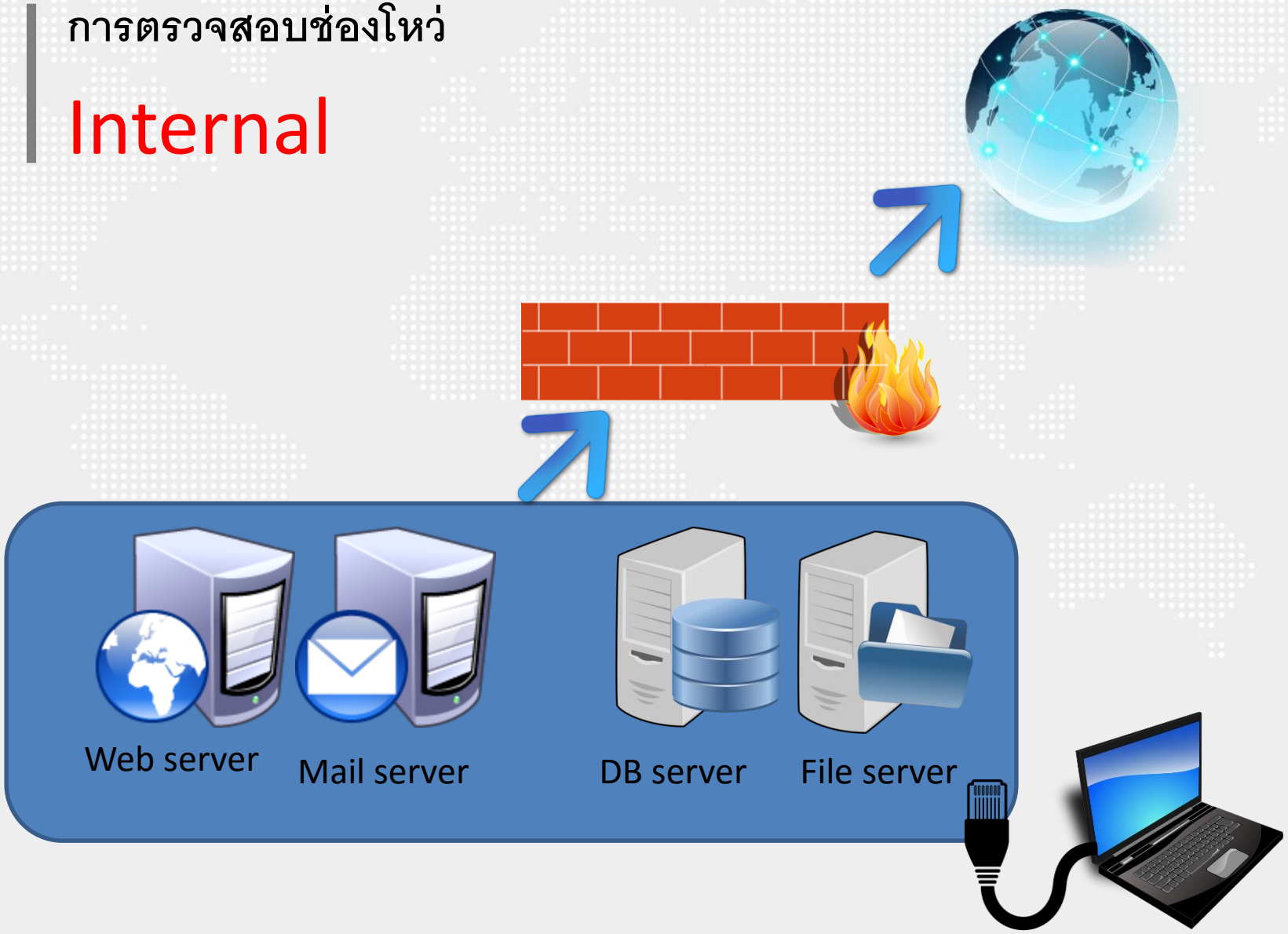
ระดับความเสี่ยง **(Information)**

ความเสี่ยงระดับต่ำ (Information) เป็นข้อมูลพื้นฐานทั้งหมดของระบบ ผู้โจมตีไม่สามารถโจมตีช่องโหว่ระดับนี้ได้

(CVSS Score 0 – 2.9)

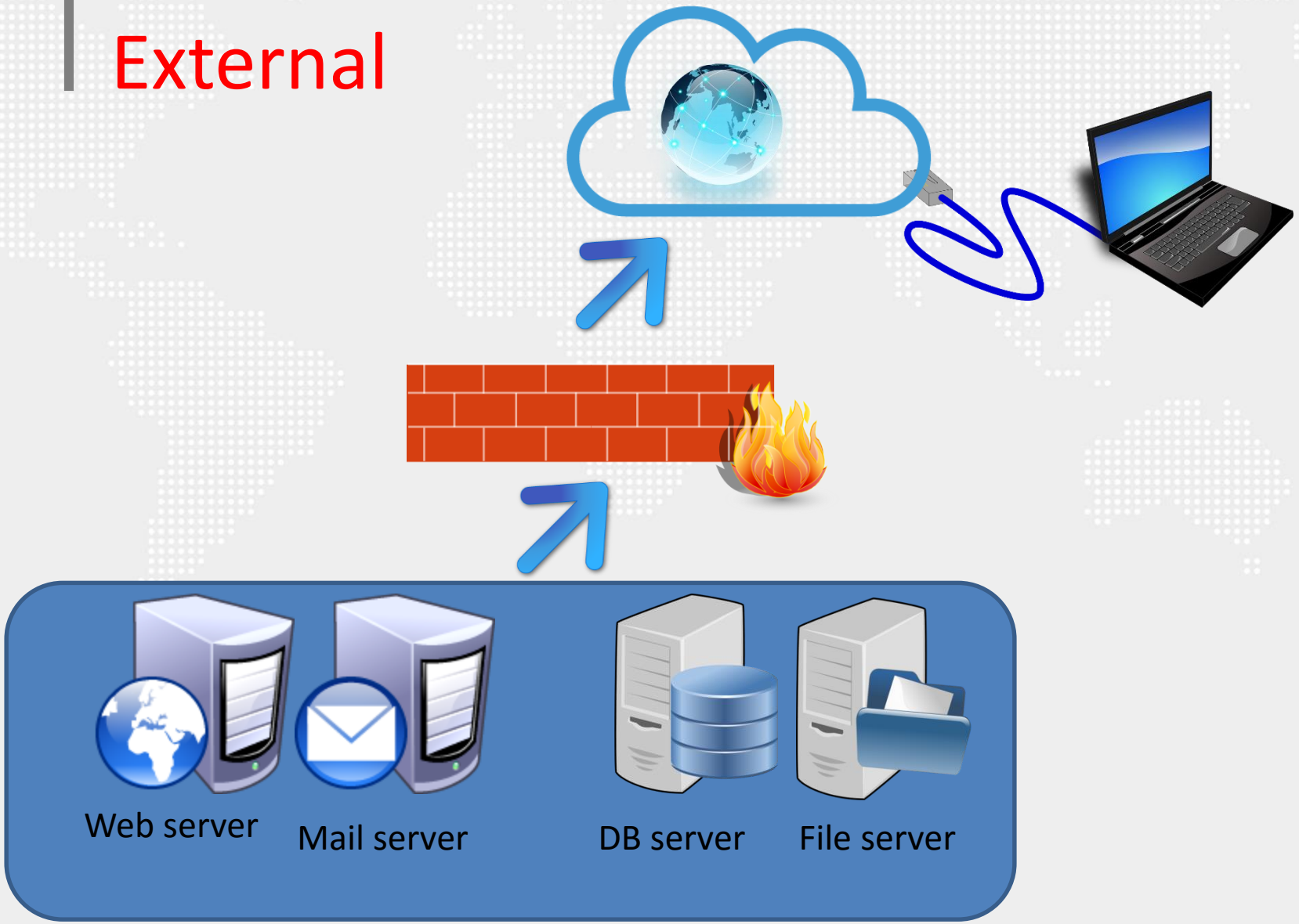
การตรวจสอบช่องโหว่

Internal



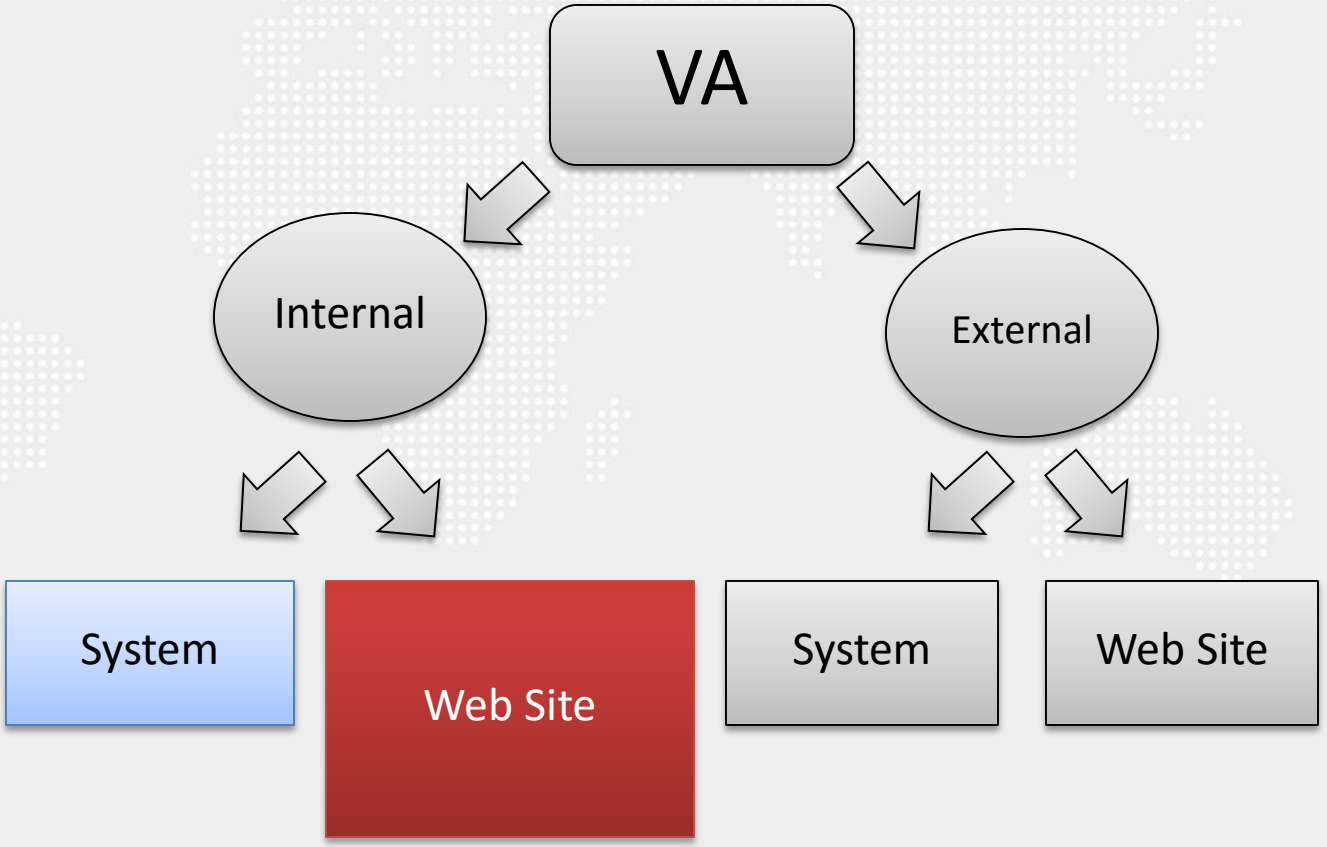
การตรวจสอบช่องโหว่

External



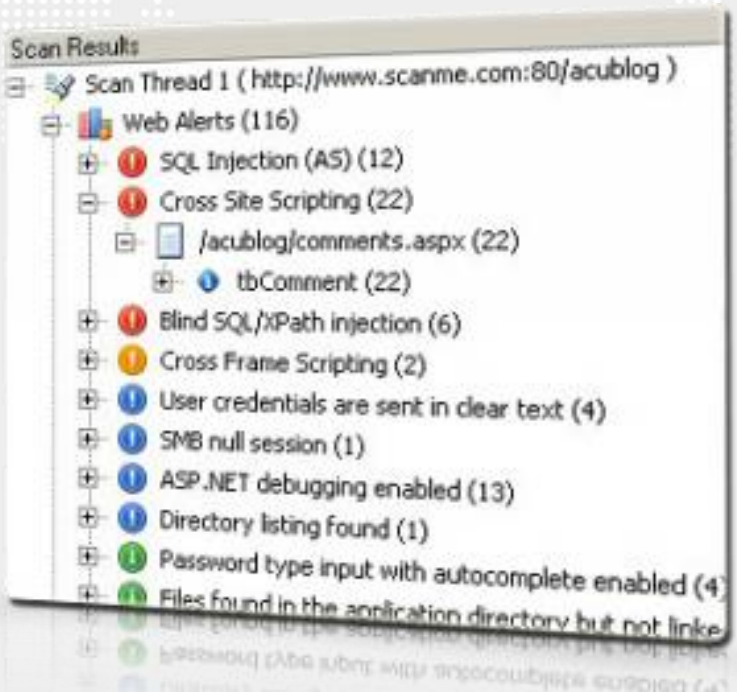
การตรวจสอบช่องโหว่

(Web site)



การตรวจสอบช่องโหว่ acunetix

(WEB Site)



การตรวจสอบช่องโหว่

OWASP Top 10 – 2013 (New)

OWASP
Open Web Application Security Project

A1 – Injection
A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control
A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards

https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013
https://www.facebook.com/groups/owaspthailand/

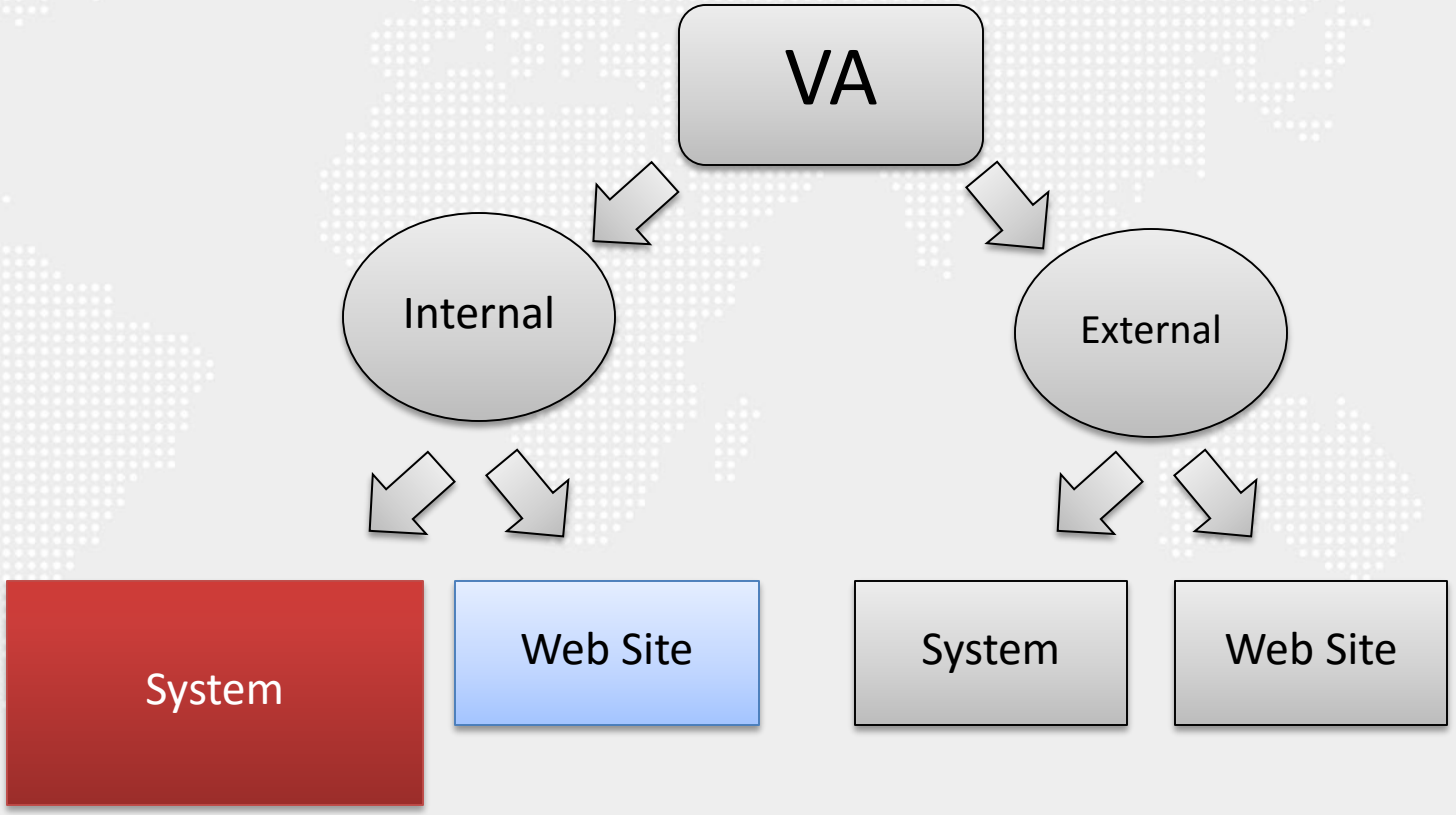
การตรวจสอบช่องโหว่

Web Application Scanner tools

Acunetix WVS by Acunetix
AppScan by IBM
Burp Suite Professional by PortSwigger
Hailstorm by Cenzic
N-Stalker by N-Stalker
Nessus by Tenable Network Security
NetSparker by Mavituna Security
NeXpose by Rapid7
NTOSpider by NTObjectives
ParosPro by MileSCAN Technologies
Retina Web Security Scanner by eEye Digital Security
WebApp360 by nCircle
WebInspect by HP
WebKing by Parasoft
Websecurify by GNUCITIZEN

การตรวจสอบช่องโหว่

(Web site)

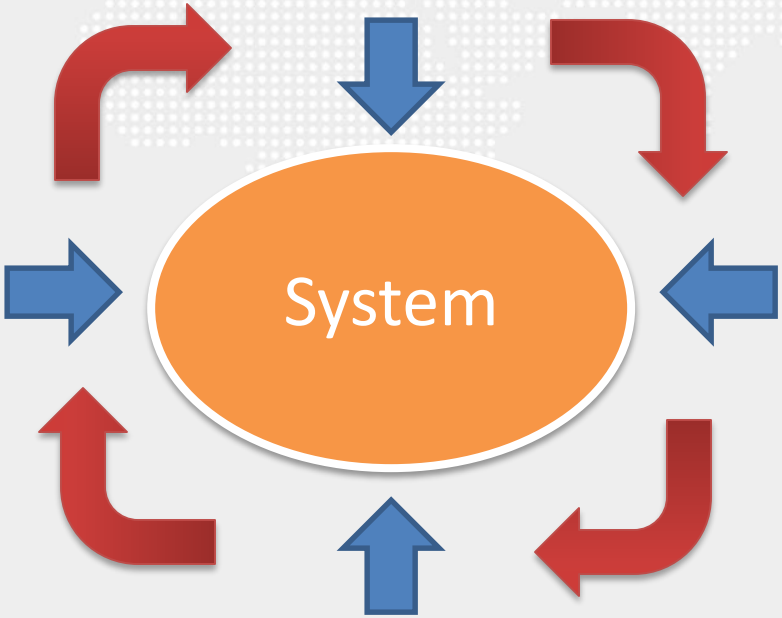


การตรวจสอบช่องโหว่

System Vulnerability

Operating System
Microsoft Windows
Solaris
Ubuntu Linux
OSX ,IOS , Android

IP Address
172.17.12.1
203.158.144.2
61.19.12.2
xxx.xxx.xxx.xxx



Program, Version, and Configuration

IIS , Apache , PHP,ASP

Ports
21,22,53,80,88,123,161,1433,3389

การตรวจสอบช่องโหว่

Top of security tools (System)

MBSA

Vulnerability Assessment Software

Nessus®

OpenVAS
Open Vulnerability Assessment System

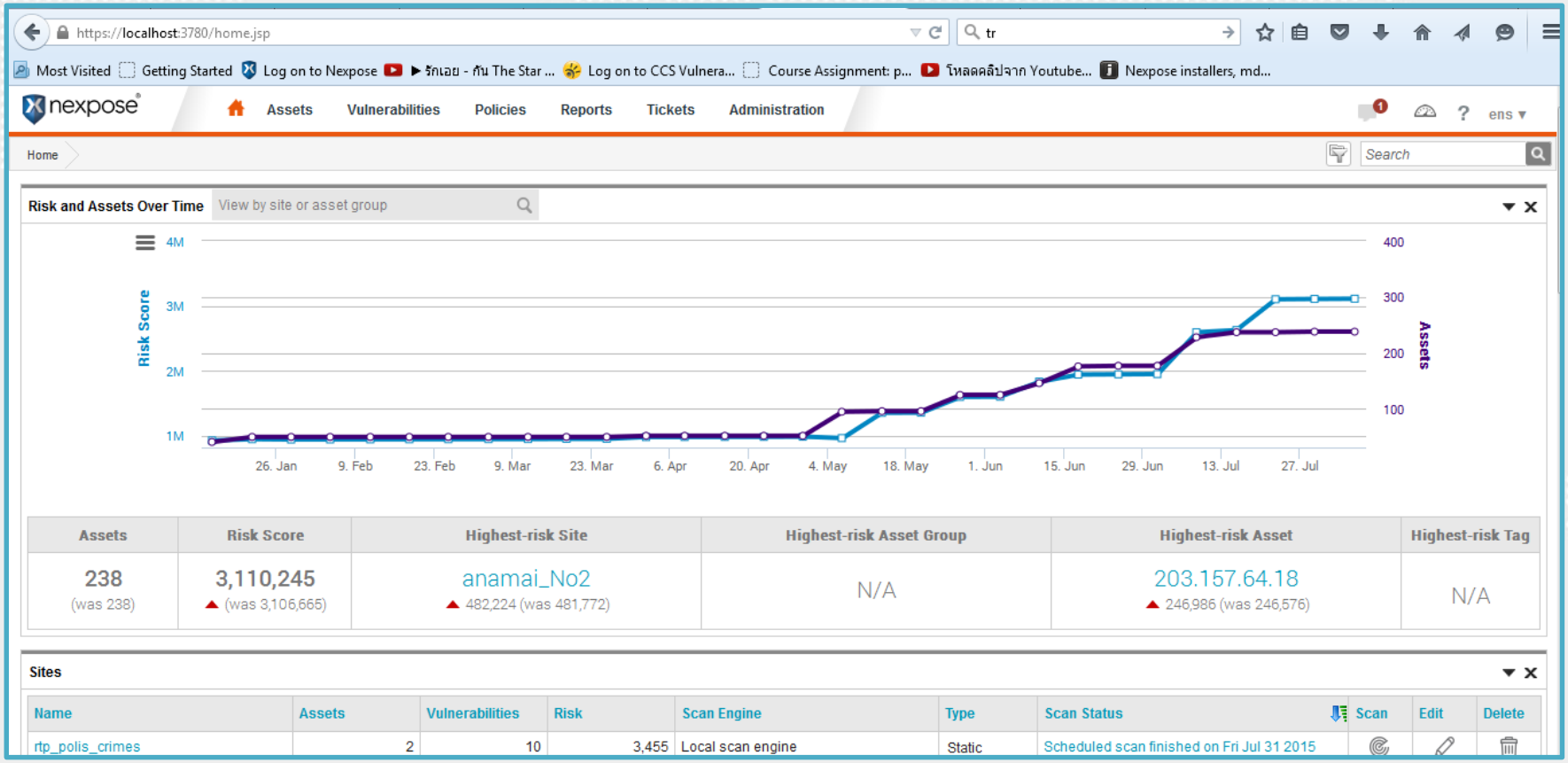
RETINA
NETWORK SCANNER

Microsoft Baseline Security Analyzer

nexpose®

GFI LanGuard™
Network security scanner and patch management

Rapid7 Nexpose



Rapid7 Nexpose

Nexpose: System Requirements
Officially Supported Systems
Minimum Hardware
2 GHz+ processor (Dual-core processor recommended)
8 GB RAM (16 GB recommended)
80 GB+ available disk space (10 GB for Community Edition)
10 GB+ available disk space for Scan engines
English operating system with English/United States regional settings
100 Mbps network interface card (1 Gbps NIC recommended)

Browsers
Google Chrome (latest) (RECOMMENDED)
Mozilla Firefox (latest)
Mozilla Firefox ESR (latest)
Microsoft Internet Explorer 9*, 10, 11

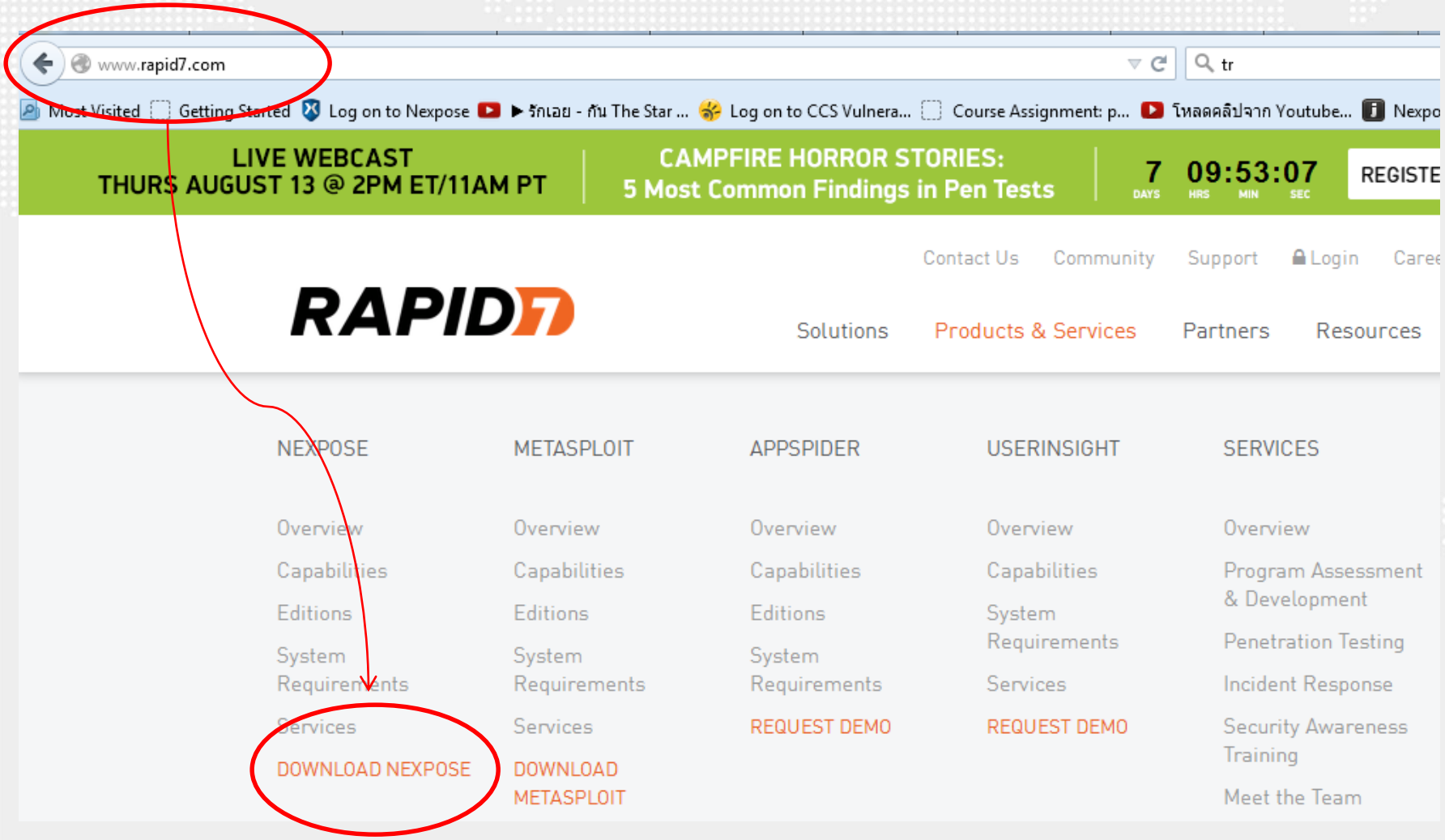
Rapid7 Nexpose

Operating Systems

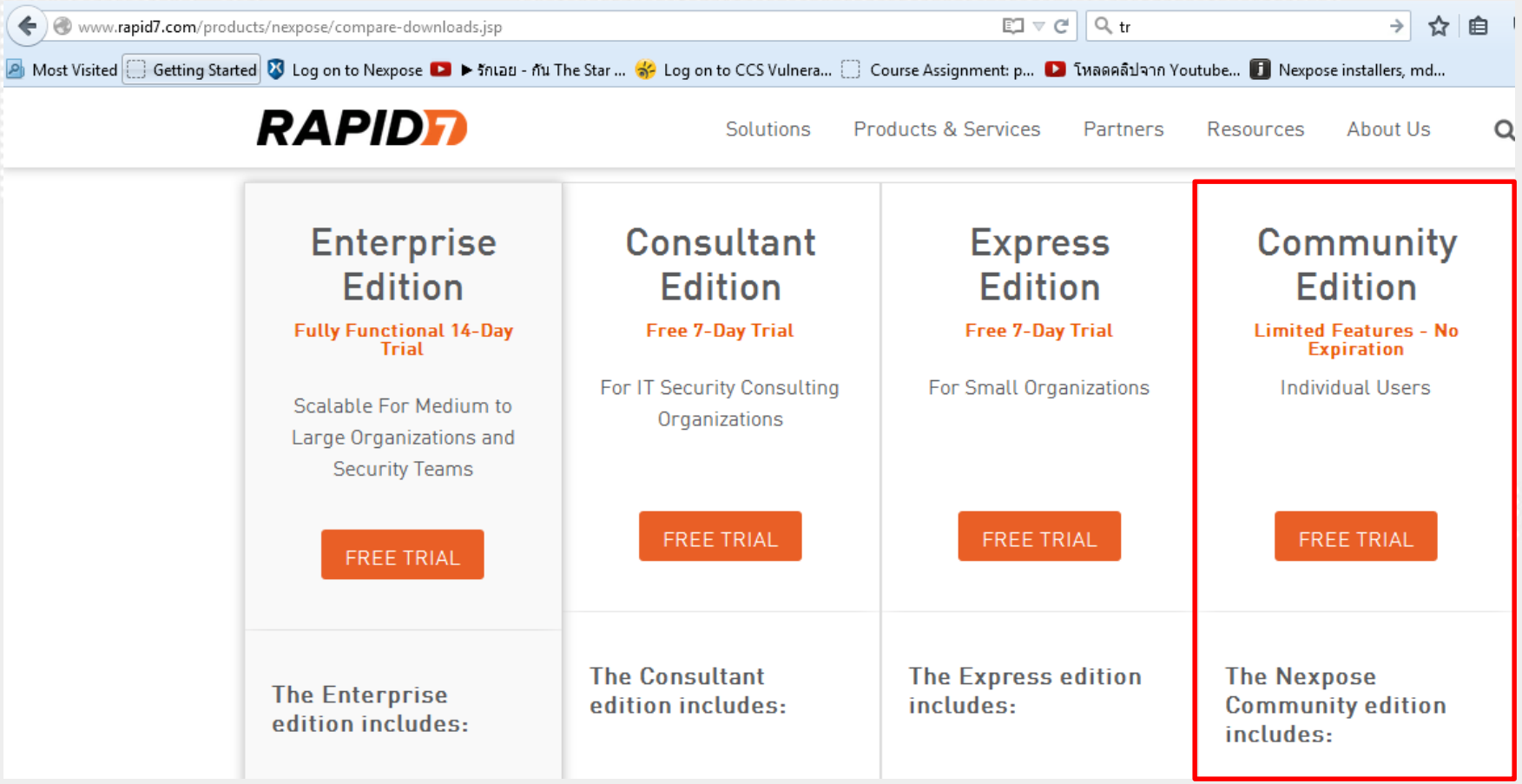
64-bit versions of the following platforms are supported.

Ubuntu Linux 12.04 LTS (RECOMMENDED)
Ubuntu Linux 14.04 LTS
Ubuntu Linux 10.04 LTS*
Microsoft Windows Server 2008 R2
Microsoft Windows Server 2012 R2
Microsoft Windows 8.1
Microsoft Windows 7 SP1+
Red Hat Enterprise Linux Server 6.5 or later
Red Hat Enterprise Linux Server 5.10 or later
Kali Linux 1.0.x
Virtual Machines on VMware ESXi 5.x, VMware vCenter Server 5.x

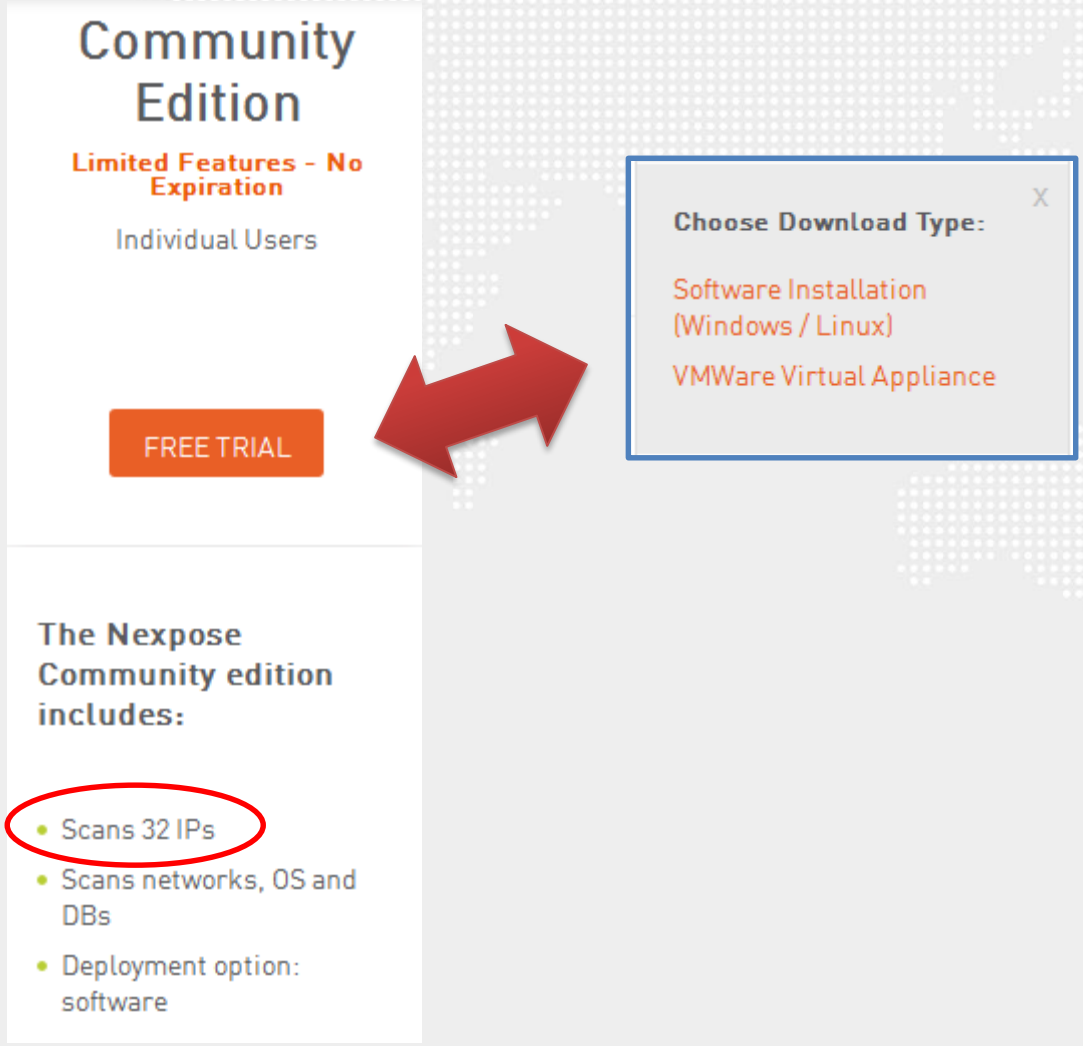
Rapid7 Nexpose



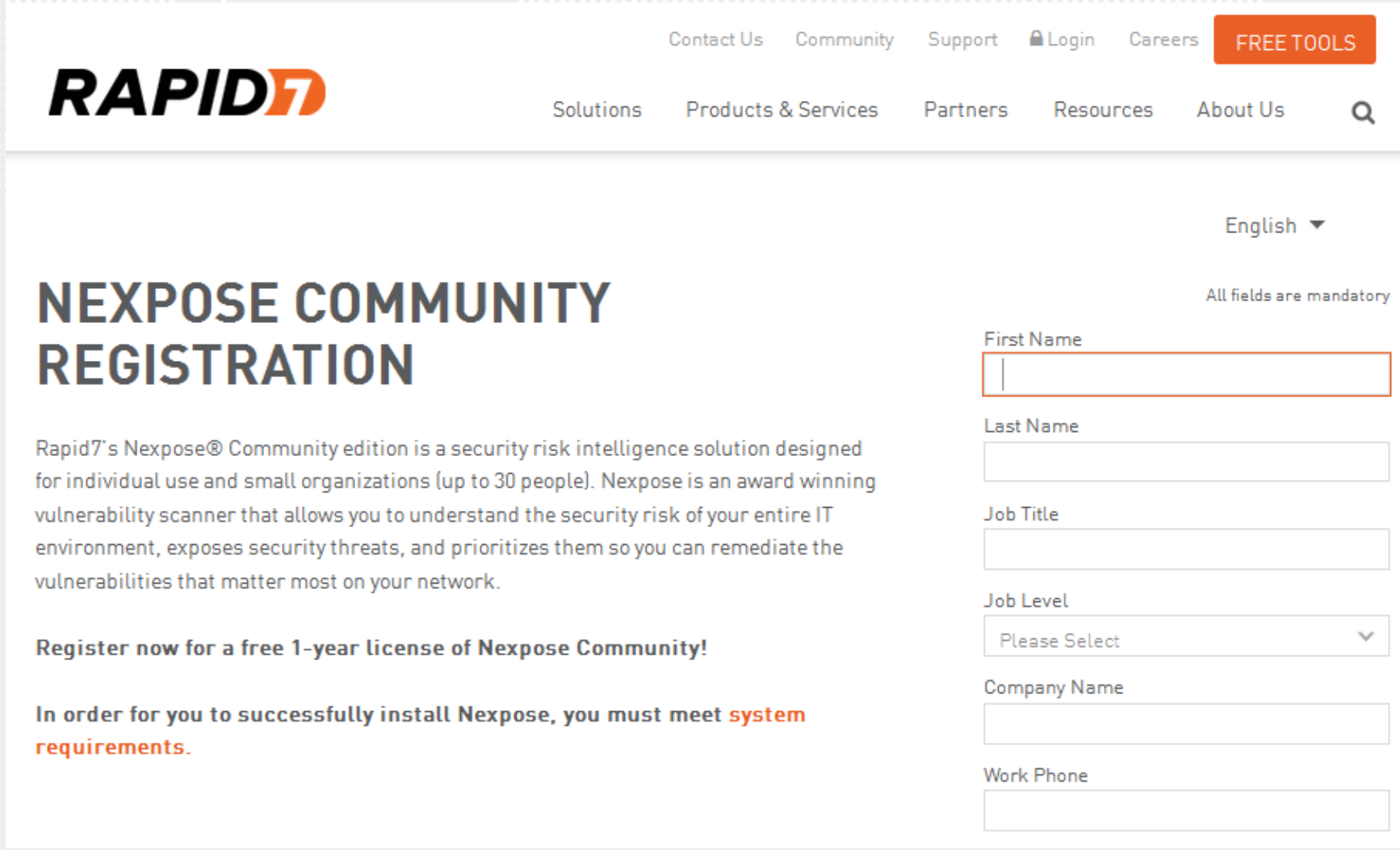
Rapid7 Nexpose



Rapid7 Nexpose



Rapid7 Nexpose



Rapid7 Nexpose

All fields are mandatory

First Name
pongrapee

Last Name
narkmanee

Job Title
en

Job Level
System/Security Admin

Company Name
ega

Work Phone
6626126000

Work Email
pongrapee@ega.or.th Change

Country
Thailand

State/ Province

Captcha
การตรวจสอบหมดอายุ เลือกช่องทำเครื่องหมายอีกครั้ง
ฉันไม่ใช่โปรแกรมอัตโนมัติ
reCAPTCHA

Read the Terms & Conditions

Yes, I accept the terms and conditions of the Rapid7 End User License Agreement

SUBMIT & DOWNLOAD

Issues with this page? Please email info@rapid7.com
Please see updated Privacy Policy

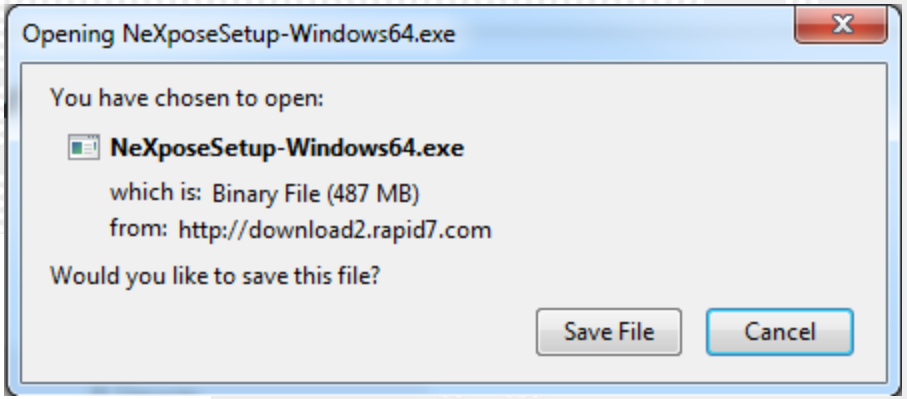
Rapid7 Nexpose

Next steps to get started with Nexpose Community

STEP 1: Download

Windows	Linux
64-Bit | md5sum	64-Bit | md5sum

Rapid7 Nexpose



STEP 2: Install

Once the download is complete, run the installer and follow the step by step instructions.

STEP 3: Activate

An email containing your license key has been sent to the email address provided on the previous registration page. Insert your license key into Nexpose to activate and unlock Nexpose Community.

Note: It may take up to 15 mins to receive your license delivery email. Please check your spam folder, if you do not receive the email or cannot find the license key in the email, contact info@rapid7.com.

Rapid7 Nexpose

จาก : Swofford, Caitlin <caitlin_swofford@rapid7.com>
หัวเรื่องจดหมาย : Your Nexpose License Key – Get Started
ถึง : pongrapee narkmanee <pongrapee@ega.or.th>
ตอบกลับ : Swofford, Caitlin <messages.663271.41651790.409e59a784@messages.netsuite.com>

M@il.Go.th
ระบบจดหมายอิเล็กทรอนิกส์กลาง เพื่อการสื่อสารในภาครัฐ

10 Minute Mail

Your Nexpose Community License Key

Rapid7

GH8Y-52PC-HM7P-7QNJ Follow the steps below to get started

Thank you for registering for Nexpose Community. **Please follow the steps below to activate your free software license.**

1. If you have not downloaded our software yet, do so here: Download Nexpose

2. After download is complete, run the installer and enter your product key to activate your license.

Your License Key: GH8Y-52PC-HM7P-7QNJ

Need Help? If you run into any problems, we will get you up and running.

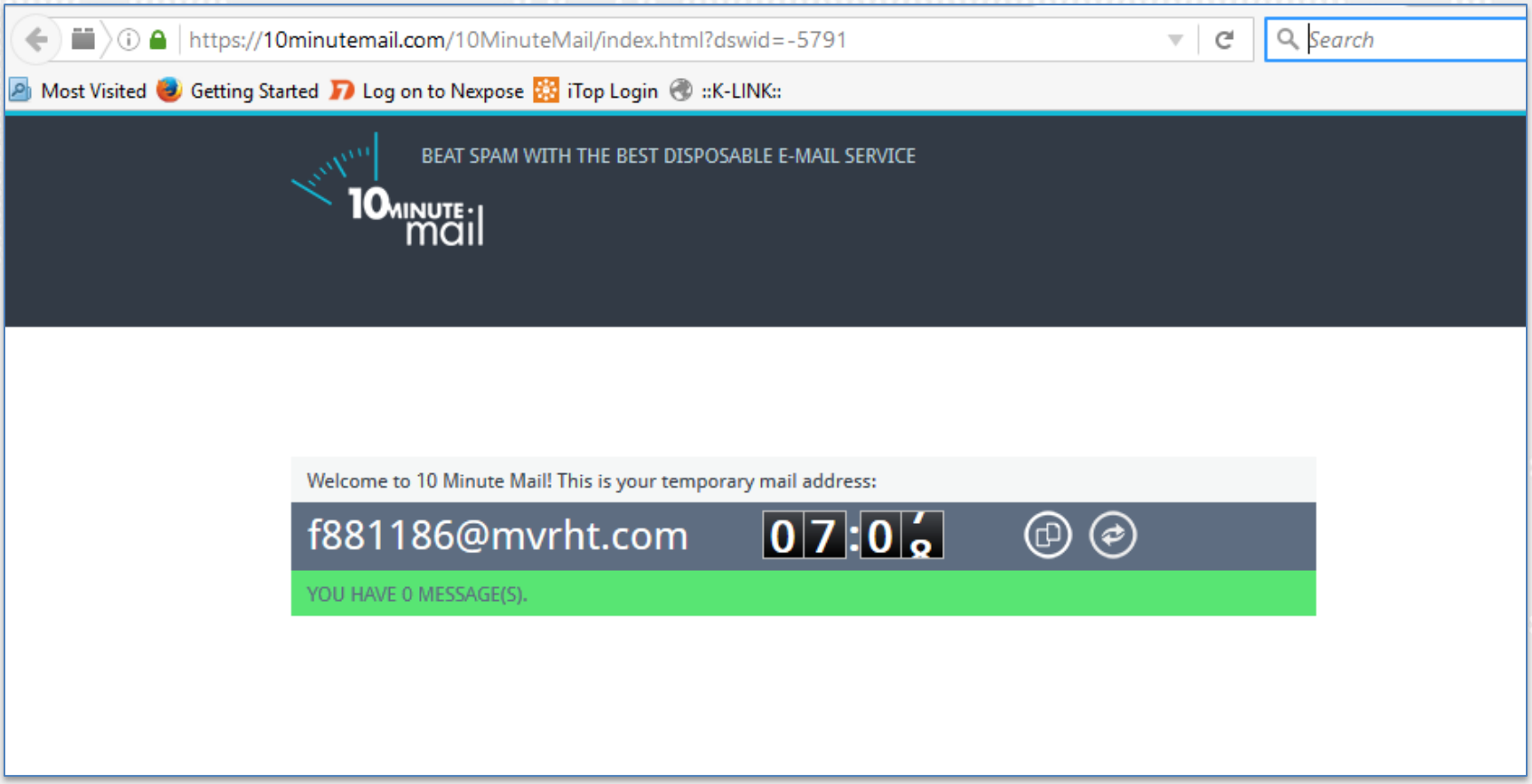
Community: Join the Nexpose Community for Support

Guide: Check out our Nexpose Quickstart Guide for further assistance

Video: Step by Step: Downloading and Activating Nexpose

We hope you enjoy Nexpose.

https://10minutemail.com/

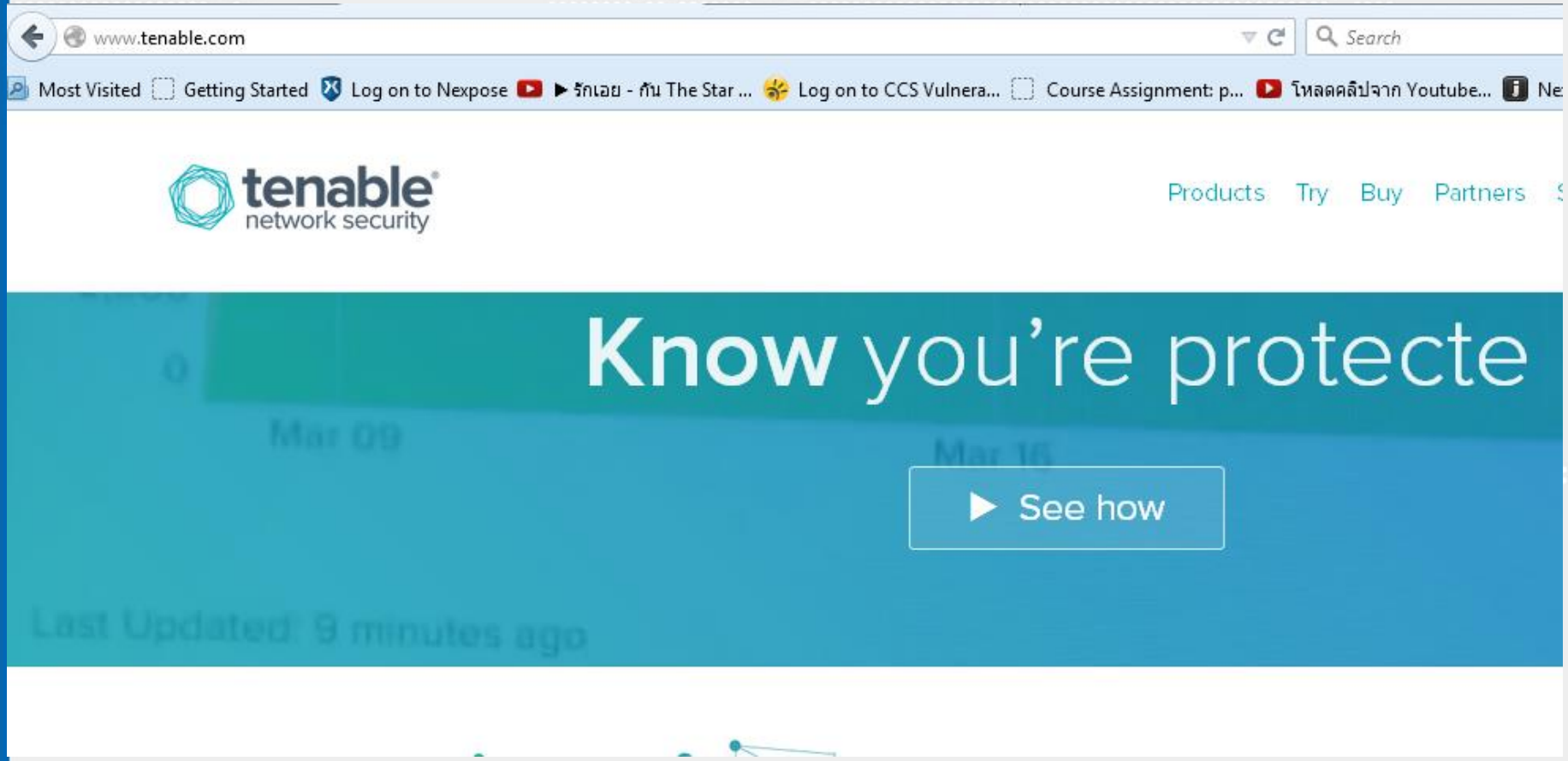


Vulnerability Assessment

tenable network security

EGA e-Government Agency THAILAND

Nessus

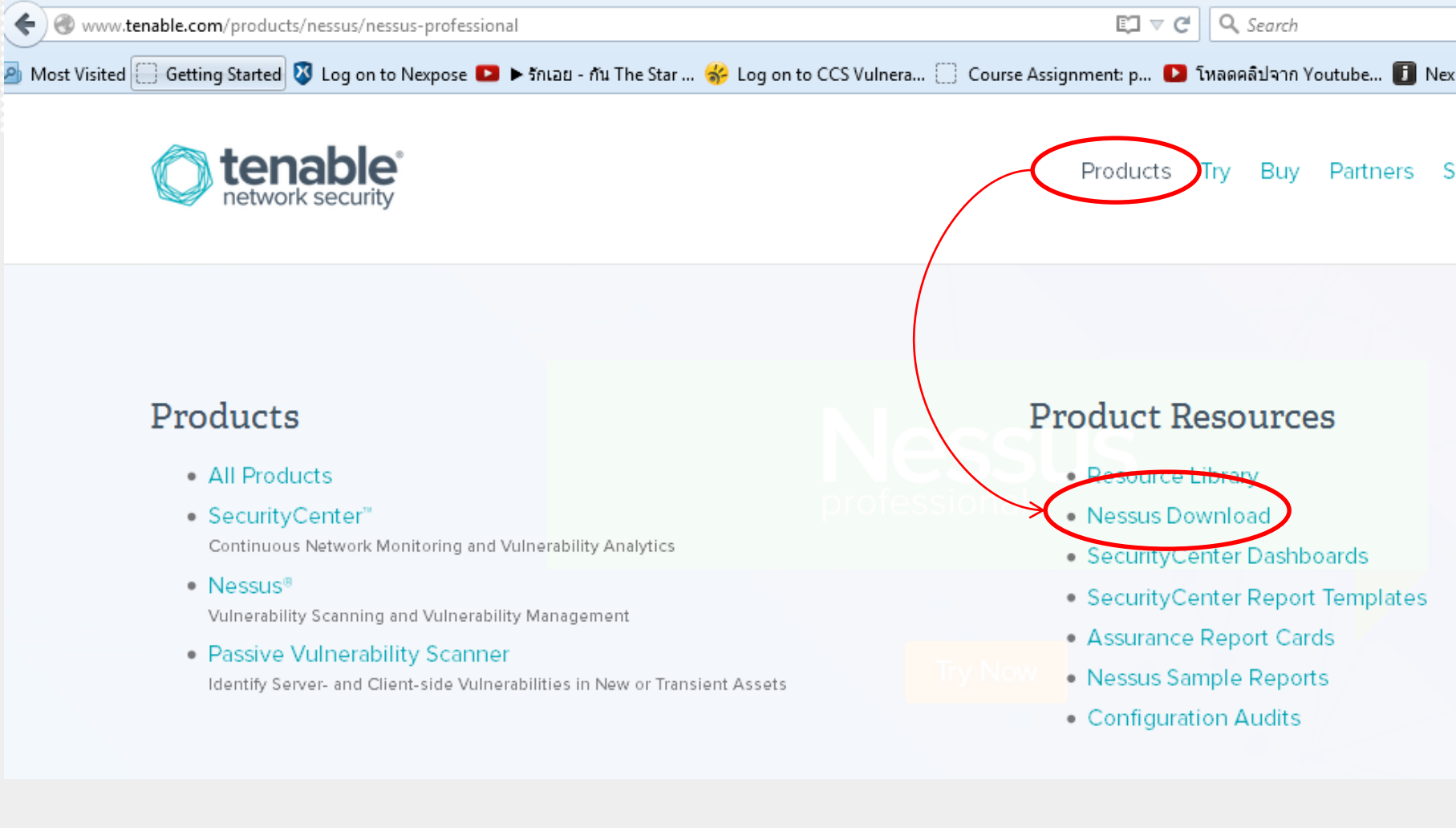


Vulnerability Assessment

tenable network security

EGA e-Government Agency THAILAND

Nessus



Vulnerability Assessment

tenable network security

EGA e-Government Agency THAILAND

Nessus

	Nessus Home	Nessus Professional	Nessus Manager	Nessus Cloud
What it does	Vulnerability scanning Download	Vulnerability scanning Download	Vulnerability management Request an Evaluation	Cloud hosted vulnerability management Request an Evaluation
Designed For	Home use only	Single users, commercial	Multiple users, commercial	Multiple users, commercial
Standard evaluation timeframe	Unlimited	7 days	14 days	14 days
		Buy	Buy	Buy

Vulnerability Assessment

tenable network security

EGA e-Government Agency THAILAND

Nessus

Please Select Your Operating System

- Microsoft Windows
- Mac OS X
- Linux
- FreeBSD
- GPG Keys

Vulnerability Assessment

tenable network security

EGA e-Government Agency THAILAND

Nessus

Please Select Your Operating System

- Microsoft Windows

Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, and 8 (64-bit)
File: Nessus-6.4.3-x64.msi
MD5: b81cfca4c785cab33dab8f164fba1288

Windows Server 7, and 8 (32-bit)
File: Nessus-6.4.3-Win32.msi
MD5: 71bc7e2152d8621e5413243d1ab4cbae

- Mac OS X
- Linux
- FreeBSD
- GPG Keys

Vulnerability Assessment

Subscription Agreement

TENABLE NETWORK SECURITY, INC.
NESSUS®
SOFTWARE LICENSE AND SUBSCRIPTION AGREEMENT

This is a legal agreement ("Agreement") between Tenable Network Security, Inc., a Delaware corporation having offices at 7021 Columbia Gateway Drive, Suite 500, Columbia, MD 21046 ("Tenable"), and you ("You"), the party licensing Software and/or downloading the Plugins through Tenable's subscription service (as each capitalized term is defined below). This Agreement covers Your permitted use of the Software and/or the Plugins, as applicable

These technology and/or software were licensed in accordance with the US Department of Commerce Export Administration Regulations (EAR) found at 15 CFR Parts 730 et seq. Diversion contrary to US law is prohibited. No physical or computational access by nationals of any country listed in Country Group E:1 in Supplement No. 1 to part 740 of the EAR (including Cuba, Iran, N. Korea, Sudan, or Syria) is permitted.

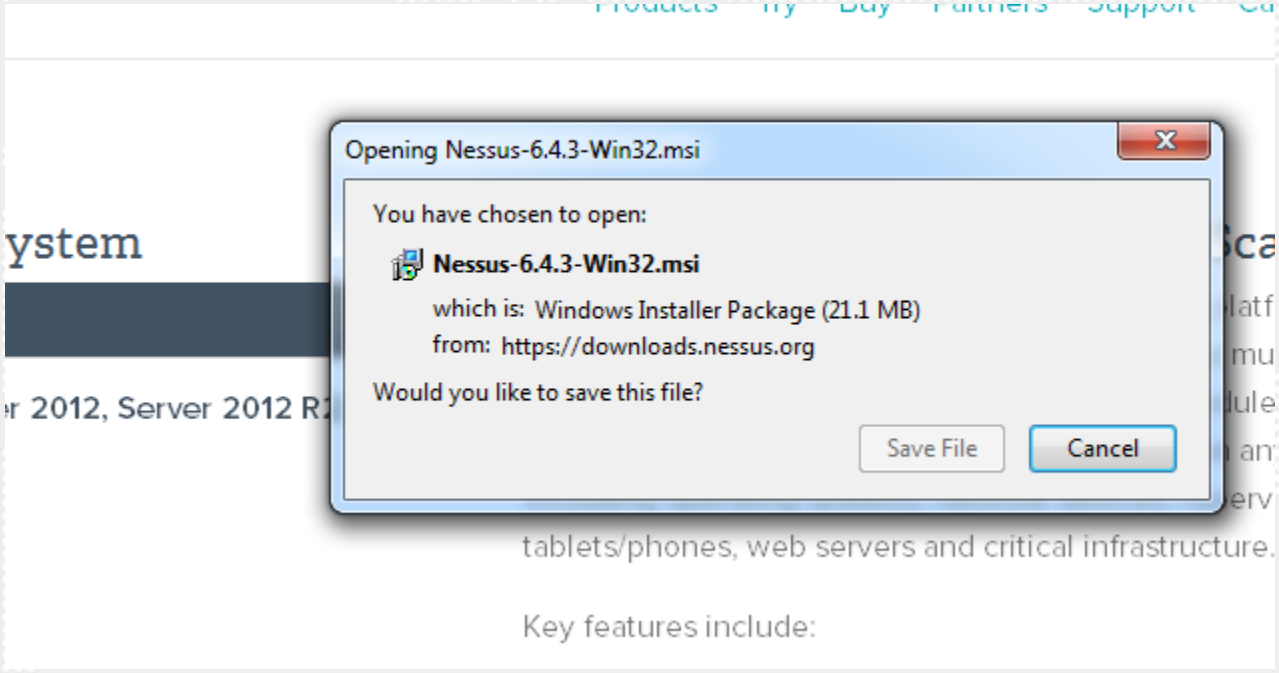
Agree

Vulnerability Assessment

tenable network security

EGA e-Government Agency THAILAND

Nessus



ทดสอบ Scan ช่องโหว่

กระบวนการ Vulnerability Management สรอ.

JANUARY 2016

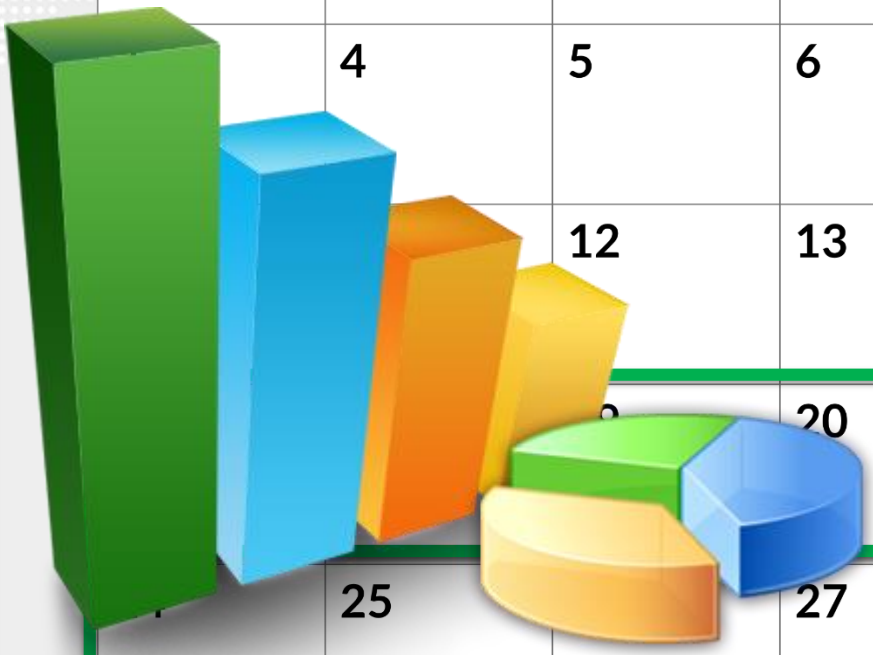
Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
					1	2
3	4	5		7	8	9
10	11	12		14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

My Calendar Land – www.mycalendarland.com

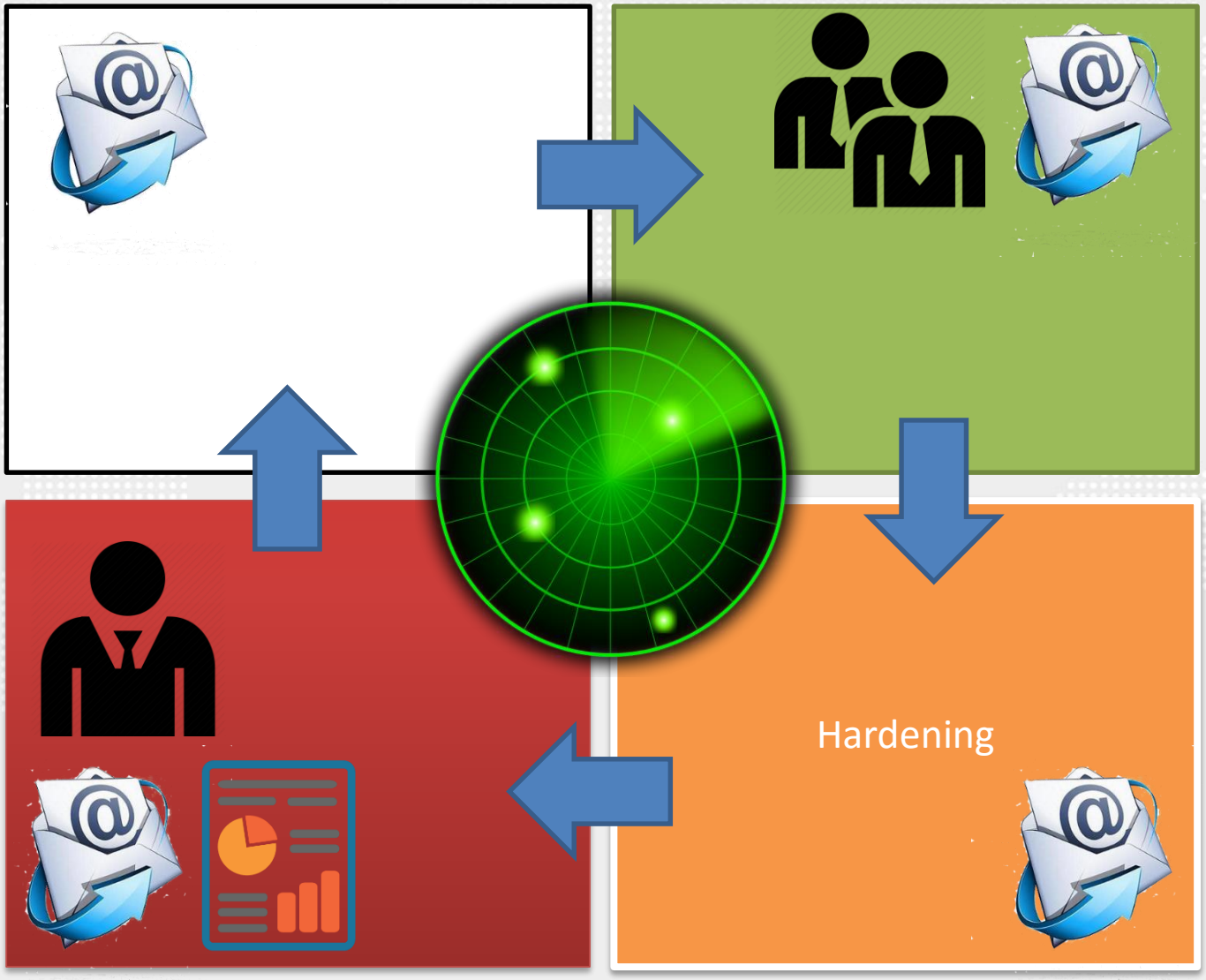
กระบวนการ Vulnerability Management สรอ.

JANUARY 2016

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
					1	2
	4	5	6	7	8	9
		12	13	14	15	16
			20	21	22	23
	25		27	28	29	30
31						



กระบวนการ Vulnerability Management สรอ.



Email Report

Audit Report

Site of [redacted]

Audited on August 13, 2014

Reported on August 14, 2014

Email Report

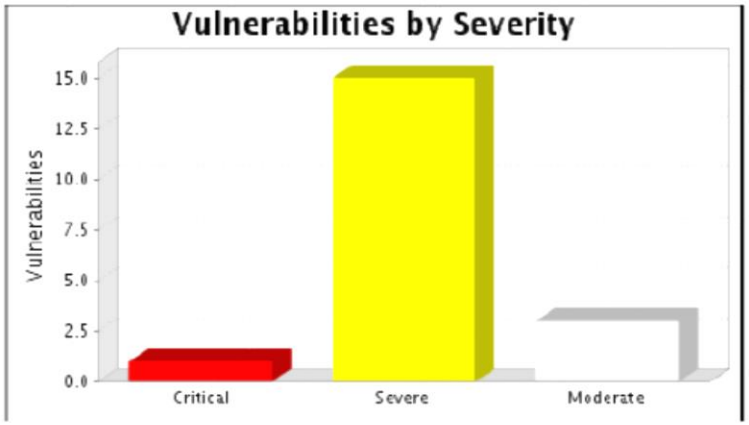
1. Executive Summary

This report represents a security audit performed by Nexpose from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

Site Name	Start Time	End Time	Total Time	Status
[redacted]	August 13, 2014 03:14, GMT	August 14, 2014 13:44, GMT	1 days 10 hours 29 minutes	Success

There is not enough historical data to display overall asset trend.

The audit was performed on one system which was found to be active and was scanned.



There were 19 vulnerabilities found during this scan. One critical vulnerability was found. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 15 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 3 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities.

Email Report

Audit Report

2. Discovered Systems

Node	Operating System	Risk	Aliases
172.17.17.119	Microsoft Windows Server 2008 R2, Standard Edition SP1	4,773	•WIN-AC75QSO1CLR

Email Report

3. Discovered and Potential Vulnerabilities

The information in this section is based on filtered vulnerability data. View the filters in the following table.

Filter	Setting
Vulnerability severity levels included	Critical and severe

3.1. Critical Vulnerabilities

3.1.1. PHP Vulnerability: CVE-2014-3515 (php-cve-2014-3515)

Description:

The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.

Affected Nodes:

Affected Nodes:	Additional Information:
172.17.17.119:80	Running HTTP serviceProduct IIS found in fingerprint is not HTTPDProduct IIS exists -- Microsoft IIS 7.5Vulnerable version of component PHP found -- PHP 5.4.24

Email Report

Vulnerability Solution:

- Upgrade to PHP version 5.4.30

  Download and apply the upgrade from: http://www.php.net/releases/

- Upgrade to PHP version 5.5.14

  Download and apply the upgrade from: http://www.php.net/releases/

การตรวจสอบช่องโหว่ของผู้โจมตีระบบ

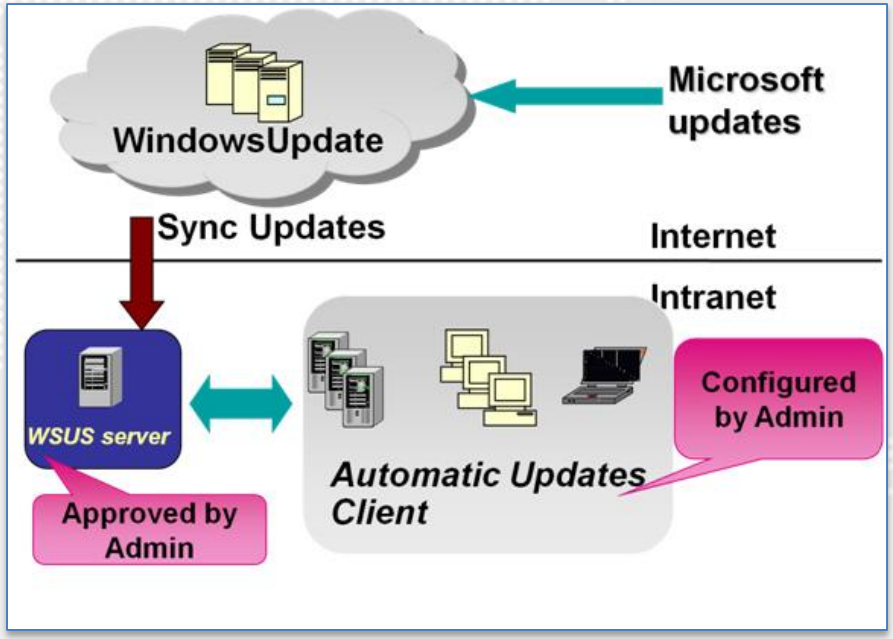
Passive Scan

Active Scan

การดำเนินการหลังการ VA

ปิดช่องโหว่ Hardening

- Update Services Pack and Patch
- Upgrade Programs
- Update Configure
- Disable Unused Services



การสร้างความปลอดภัยให้ระบบตั้งแต่เริ่มต้น

Hardening System

Hardening OS

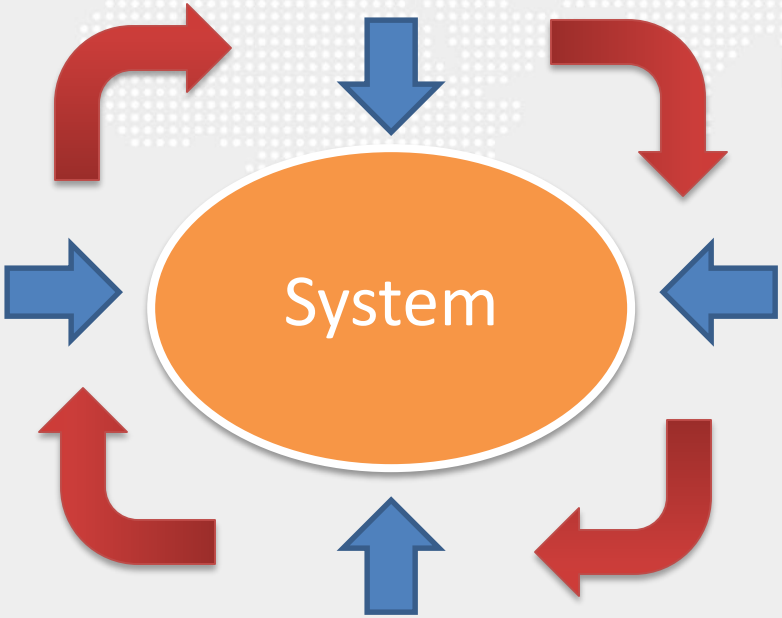
Operating System

Microsoft Windows
Solaris
Ubuntu Linux
OSX ,IOS , Android

Hardening Program

IP Address

172.17.12.1
203.158.144.2
61.19.12.2
xxx.xxx.xxx.xxx



Program, Version, and Configuration

IIS , Apache , PHP,ASP

Ports

21,22,53,80,88,123,161,1433,3389

Vulnerability Assessment

QUESTION & ANSWER SESSION

Name พงศ์ระพี นาคมณี [Information Security Engineer]

e-mail : pongrapee@ega.or.th tel. : 02-612-6000(4303)

Thank You

Electronic Government Agency (Public Organization)

website : www.ega.or.th
e-mail : helpdesk@ega.or.th
Tel. : (+66) 0 2612 6000
Hotline : (+66) 0 2612 6060